

# The Quantitative Risk of Oil Tanker Groundings

by

Michael D. Amrozowicz

B.S. Electrical Engineering (High Honors)  
University of Florida, 1990

SUBMITTED TO THE DEPARTMENT OF OCEAN ENGINEERING IN PARTIAL FUL-  
FILLMENT OF THE REQUIREMENTS FOR THE DEGREES OF

NAVAL ENGINEER

and

MASTER OF SCIENCE IN OCEAN SYSTEMS MANAGEMENT

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 1996

©1996 Michael D. Amrozowicz. All rights reserved.

The author hereby grants to MIT permission to reproduce  
and to distribute publicly paper and electronic  
copies of this thesis document in whole or in part.

Signature of Author: \_\_\_\_\_

Department of Ocean Engineering  
May 10, 1996

Certified by: \_\_\_\_\_

Michael Golay  
Professor of Nuclear Engineering  
Thesis Advisor

Certified by: \_\_\_\_\_

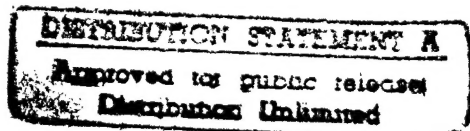
Alan Brown  
Professor of Naval Architecture  
Thesis Supervisor

Accepted  
by: \_\_\_\_\_

A. Douglas Carmichael  
Chairman, Committee for Graduate Studies

DTIC QUALITY INSPECTED 3

19961018 045





# **The Quantitative Risk of Oil Tanker Groundings**

by

Michael D. Amrozowicz

Submitted to the Department of Ocean Engineering  
on May 10, 1996 in Partial Fulfillment of the  
Requirements for the Degrees of  
Naval Engineer  
and  
Master of Science in Ocean Systems Management

## **Abstract**

The culture, design, and operation of the maritime industry all contribute to create an error-inducing system. As oil tankers have become larger, the tolerance for error has decreased as the consequences have increased. Highly visible oil spills have made society more aware of the dangers inherent with transporting oil at sea. Tankers are the largest contributor by vessel type to worldwide oil spill volume.

Human error has consistently been attributed to 80 percent of the marine accidents, a closer look reveals that many accidents attributed to human error are system errors. In fact, the term human error is unwarranted in many high-risk accidents and its use is a pejoration of the context. It points more to the action as an independent clause, rather than the context in which the action takes place.

The maritime industry has been identified as a high risk operation, requiring an active risk management program. Yet, to effect the appropriate risk management program, there must be an appreciation for the risk at hand. A probabilistic risk assessment (PRA) provides a formal process of determining the full range of possible adverse occurrences, probabilities, and expected costs for any undesirable event. A PRA can identify those areas that offer the greatest risk-reducing potential.

This thesis focuses on the first level of a proposed three-level risk model to determine the probability of a tanker grounding. The approach utilizes fault trees and event trees and incorporates The Human Error Rate Prediction data to quantify individual errors. The result allows the identification of high-leverage factors in order to determine the most effective and efficient use of resources to reduce the probability of grounding; showing that the development of the Electronic Chart Display and Information System incorporated with the International Safety Management Code can significantly reduce the probability of grounding.

Thesis Supervisor: Alan Brown  
Title: Professor of Naval Architecture

# Table of Contents

<b>Abstract .....</b>	<b>3</b>
<b>Table of Contents .....</b>	<b>5</b>
<b>List of Tables .....</b>	<b>6</b>
<b>List of Figures.....</b>	<b>7</b>
<b>Chapter 1 Introduction .....</b>	<b>8</b>
1.1 The Motivation .....	8
1.2 The Approach .....	10
1.3 Discussion.....	11
1.4 Outline.....	12
<b>Chapter 2 The Nature of the Problem .....</b>	<b>13</b>
2.1 The Tanker Problem .....	13
2.2 Oil Spill Data.....	16
2.3 Summary .....	19
<b>Chapter 3 Risk Assessment .....</b>	<b>21</b>
3.1 The Probabilistic Risk Assessment .....	21
3.2 Fault Trees.....	22
3.2.1 Fault Tree Evaluation .....	23
3.3 Event Trees.....	25
3.3.1 Event Tree Evaluation .....	25
3.4 The Grounding Fault Tree.....	27
3.5 Summary .....	29
<b>Chapter 4 The Human Problem .....</b>	<b>30</b>
4.1 The Importance of the Human Problem.....	30
4.1 The Historical Pervasiveness.....	30
4.3 Human Failure and Individual Error .....	31
4.4 Accident Investigations .....	33
4.5 The Pathogen Metaphor .....	34
4.6 Accident Causation .....	34
4.6.1 Design and Construction.....	35
4.6.2 Operations .....	36
4.7 The Dynamics of Accident Causation.....	39
4.8 Technology and Risk Homeostasis .....	40
4.9 Summary .....	42
<b>Chapter 5 Human Reliability Analysis .....</b>	<b>44</b>
5.1 Methodology .....	44
5.2 THERP .....	44
5.2.1 Define System Failures of Interest.....	45
5.2.2 List and Analyze Related Human Actions .....	45
5.2.3 Estimate Relevant Error Probabilities.....	46
5.2.4 Estimate the Effects of Error on System Failure Events.....	47
5.2.5 Recommend Changes to System Design.....	47
5.3 PSFs .....	48
5.3.1 PSF Considerations.....	50
5.3.2 PSF Synopsis .....	54
5.4 THERP Critics .....	55
5.5 Summary .....	55



<b>Chapter 6 Probability Determination.....</b>	<b>57</b>
6.1 The Grounding Fault Tree.....	57
6.1.1 The Emphasis on Powered Grounding .....	59
6.2 Powered Grounding .....	60
6.2.1 Passage Planning.....	61
6.2.2 Planning Information.....	66
6.2.2 Piloting.....	68
6.3 Drift Grounding.....	77
6.3.1 Wind and Current.....	78
6.3.2 Rescue and Assistance .....	78
6.3.3 Anchor Failure .....	80
6.3.4 Lost Way .....	82
6.4 Summary of Probabilities .....	84
6.5 Fault Tree Reduction.....	85
6.5.1 Powered Grounding Fault Tree Reduction.....	85
6.5.2 Drift Grounding Fault Tree Reduction .....	86
6.6 The Probability of Grounding.....	87
6.7 Summary .....	87
<b>Chapter 7 Evaluations and Conclusions.....</b>	<b>89</b>
7.1 High-Leverage Factors.....	89
7.2 Powered Grounding Sensitivity Analysis.....	89
7.2.1 Planning Failure Sensitivity.....	89
7.2.2 Piloting Failure Sensitivity.....	90
7.3 Recommendations.....	92
7.3.1 Sub-System Improvements.....	92
7.3.2 Organizational and Procedural Improvements.....	93
7.4 Conclusions .....	94
7.5 Areas for Further Research.....	95
<b>Appendix A Boolean Algebra and Probability Theory .....</b>	<b>96</b>
<b>Appendix B Developing the Grounding Fault Tree .....</b>	<b>100</b>
<b>Appendix C Selected THERP Tables.....</b>	<b>108</b>
<b>Appendix D Sensitivity Calculations .....</b>	<b>110</b>
<b>Bibliography .....</b>	<b>119</b>

## List of Tables

TABLE 2 - 1: REGISTERED TONNAGE (VESSELS GREATER THAN 1000 DWT) IN PRINCIPAL FOCs (STATUS: DECEMBER 31, 1993).....	13
TABLE 2 - 2: NUMBER OF LOSSES AND GROSS TONNAGE LOST FROM 1988 - 1992 (VESSELS > 500 GROSS TONS) .....	14
TABLE 2 - 3: SELECTED MAJOR OIL SPILLS.....	18
TABLE 2 - 4: FIVE LARGEST TANKER SPILLS 1993-1994.....	18
TABLE 5 - 1: PERFORMANCE SHAPING FACTORS .....	49
TABLE 6 - 1: HEPs FOR PASSAGE PLANNING.....	63
TABLE 6 - 2: HEP FOR RECOGNIZING FAULTY TRACK.....	65
TABLE 6 - 3: ANNUAL VESSEL TRIPS FOR SELECTED PORTS.....	67
TABLE 6 - 4: INCORRECT PLANNING INFORMATION ACCIDENT QUOTIENTS .....	68
TABLE 6 - 5: HEPs FOR PILOTING .....	70
TABLE 6 - 6: HEPs FOR VERIFICATION ROLE .....	71
TABLE 6 - 7: SUMMARY OF PILOTING FAILURE PROBABILITIES FOR VARYING LEVELS OF VERIFICATION.....	74
TABLE 6 - 8: TANKER-TUG GROUNDING ACCIDENTS.....	80
TABLE 6 - 9: ANCHOR FAILURE ACCIDENT QUOTIENT.....	81
TABLE 6 - 10: LOST WAY ACCIDENT QUOTIENTS .....	83
TABLE 6 - 11: APPROXIMATE COASTAL TRANSIT LENGTH (MILES).....	83
TABLE 6 - 12: LOST WAY FAILURES PER MILE.....	83
TABLE 6 - 13: SUMMARY OF GROUNDING PROBABILITIES.....	85
TABLE 7 - 1: PLANNING FAILURE EVENT TREE HIGH-LEVERAGE FACTORS.....	89
TABLE 7 - 2: PLANNING FAILURE EVENT TREE (INCORPORATING THE PROBABILITY FOR FAULTY INFORMATION) HIGH-LEVERAGE FACTORS .....	90
TABLE 7 - 3: PILOTING FAILURE EVENT TREE HIGH-LEVERAGE FACTORS (INCORPORATING CAPTAIN'S VERI- FICATION ROLE) .....	91
TABLE 7 - 4: PILOTING FAILURE EVENT TREE HIGH-LEVERAGE FACTORS (WITHOUT CAPTAIN'S VERIFICATION ROLE).....	91

## List of Figures

FIGURE 1 - 1: MARITIME OIL SPILL VOLUME BY VESSEL SERVICE.....	8
FIGURE 1 - 2: MAJOR TANKER OIL SPILLS AND CAUSES.....	9
FIGURE 1 - 3: RISK MODEL .....	10
FIGURE 2 - 1: DISTRIBUTION OF TANKER LOSSES BY YEARS OF AGE BY GROSS TONNAGE (1988 - 1992).....	14
FIGURE 2 - 2: NUMBER OF TANKER LOSSES BY AGE ( 1982 AND 1992) .....	15
FIGURE 2 - 3: ESTIMATED ANNUAL WORLD WIDE OIL SPILLED .....	16
FIGURE 2 - 4: DISTRIBUTION OF SPILLS IN U.S. WATERS AND U.S. FLAGGED VESSELS .....	17
FIGURE 2 - 5: VOLUME OF OIL SPILLED FROM MAJOR AND SMALL SPILLS IN U.S. WATERS AND BY U.S. FLAGGED VESSELS .....	17
FIGURE 2 - 6: WORLD SEABORNE TRADE BY TYPES OF CARGO .....	19
FIGURE 3 - 1: AND-GATE AND OR-GATE.....	22
FIGURE 3 - 2: FAULT TREE SYMBOLISM .....	23
FIGURE 3 - 3: EXAMPLE FAULT TREE.....	24
FIGURE 3 - 4: EVENT TREE DIAGRAM .....	26
FIGURE 3 - 5: REDUCED EVENT TREE .....	27
FIGURE 3 - 6: THE GROUNDING FAULT TREE .....	28
FIGURE 4 - 1: CONTEXT OF HUMAN FAILURES AND INDIVIDUAL ERRORS .....	32
FIGURE 4 - 2: HUMAN FAILURE TAXONOMY.....	35
FIGURE 4 - 3: EMBREY'S TAXONOMIC SYSTEM .....	38
FIGURE 4 - 4: THE DYNAMICS OF ACCIDENT CAUSATION .....	40
FIGURE 4 - 5: LAW OF UNINTENDED CONSEQUENCES .....	42
FIGURE 4 - 6: WORLD TONNAGE LOSSES 1988 - 1992.....	43
FIGURE 5 - 1: PROBABILITY DETERMINATION PROCESS .....	47
FIGURE 5 - 2: EFFECTS OF STRESSES ON PERFORMANCE .....	50
FIGURE 5 - 3: HUMAN FAILURE FACTORS.....	51
FIGURE 6 - 1: GROUNDING FAULT TREE .....	58
FIGURE 6 - 2: POWERED GROUNDING FAULT TREE.....	61
FIGURE 6 - 3: PASSAGE PLANNING EVENT TREE.....	62
FIGURE 6 - 4: PASSAGE PLANNING EVENT TREE WITH ASSOCIATED PROBABILITIES.....	64
FIGURE 6 - 5: PASSAGE PLANNING EVENT TREE INCORPORATING PLOT-WAYPOINT DEPENDENCY .....	65
FIGURE 6 - 6: PILOTING EVENT TREE .....	69
FIGURE 6 - 7: PILOTING EVENT TREE WITH ASSOCIATED PROBABILITIES.....	71
FIGURE 6 - 8: PILOTING EVENT TREE INCORPORATING A VERIFICATION EVENT.....	72
FIGURE 6 - 9: PILOTING EVENT TREE INCORPORATING CAPTAINS VERIFICATION ROLE.....	73
FIGURE 6 - 10: HYPOTHETICAL WATERWAY .....	75
FIGURE 6 - 11: PILOTING WITH RECOVERY FLOW PATH.....	75
FIGURE 6 - 12: PILOTING AND RECOVERY EVENT TREE .....	76
FIGURE 6 - 13: PILOTING UNRELIABILITY VERSUS TIME.....	77
FIGURE 6 - 14: DRIFT GROUNDING FAULT TREE .....	78
FIGURE 6 - 15: ASSISTANCE EVENT TREE .....	79
FIGURE 6 - 16: TANKER LOST WAY INCIDENTS (1981-1991).....	82
FIGURE 6 - 17: LOST WAY UNRELIABILITY VERSUS TIME .....	84
FIGURE 6 - 18: GROUNDING PROBABILITIES WITH TIME .....	87

# Chapter 1 Introduction

## 1.1 The Motivation

Maritime oil spills are a significant international environmental problem. The culture, design, and operation of the maritime industry all contribute to create an error-inducing system [42].<sup>1</sup> Too often the consequence of these errors is the release of oil into the world's waterways. Oil spills have the capacity to evoke strong public reactions because of their potential environmental, economic and health impacts. Oil is an amalgam of thousands of chemicals, and each chemical affects the marine environment in a different way [14]. The environment itself lends uncertainty into any chemical's effect. Wind, waves, current, temperature, and sunlight, all affect the ability of the oil to disperse, dissolve, and biodegrade [14]. Once an oil spill has occurred, the typical recovery rate is a modest 10 to 15 percent of the spilled oil [39]. Since oil spills are low probability-high consequence events that are, by nature, difficult to predict [66], prevention is the best response. It is the risk of an oil spill that motivates further investigation. A formal risk analysis is an important step toward prevention.

Tankers are the largest contributor by vessel type to worldwide oil spill volume. From 1986 to 1994, tankship spills accounted for 60 percent of the oil spilled from maritime sources (Figure 1-1) [8].

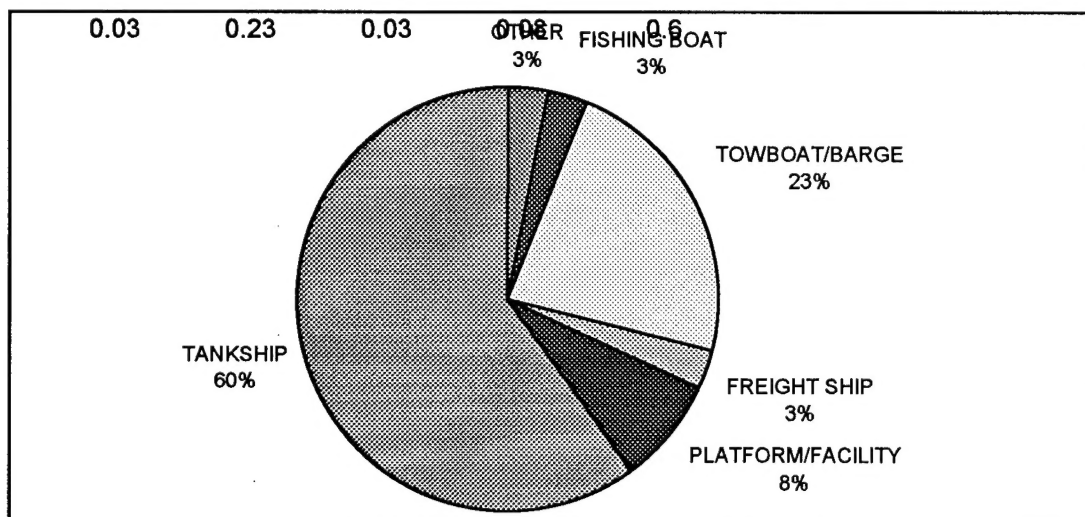


Figure 1 - 1: Maritime Oil Spill Volume by Vessel Service

<sup>1</sup> "...The [system] configuration of its many components induces errors and defeats attempts at error reduction. Discrete attempts to correct this or that will be defeated by something else; only a wholesale reconfiguration could make the parts fit together in an error-neutral or error-avoiding manner [42]."

An analysis of the claims against the United Kingdom Protection and Indemnity (UK P&I) Club in 1993 shows that tankers accounted for approximately half of total pollution claims [36].

According to the National Research Council (NRC), tanker groundings are a significant cause of oil spills (Figure 1-2) [36]. Globally, groundings represented 20 percent of all the tanker losses between 1987 and 1991 [59]. From 1981 and 1990, groundings represented 45 percent of the major spill volume in U.S. waters [29]. Therefore, groundings present a significant spill classification to investigate in order to understand how to minimize oil pollution and they will be the primary focus of this thesis.

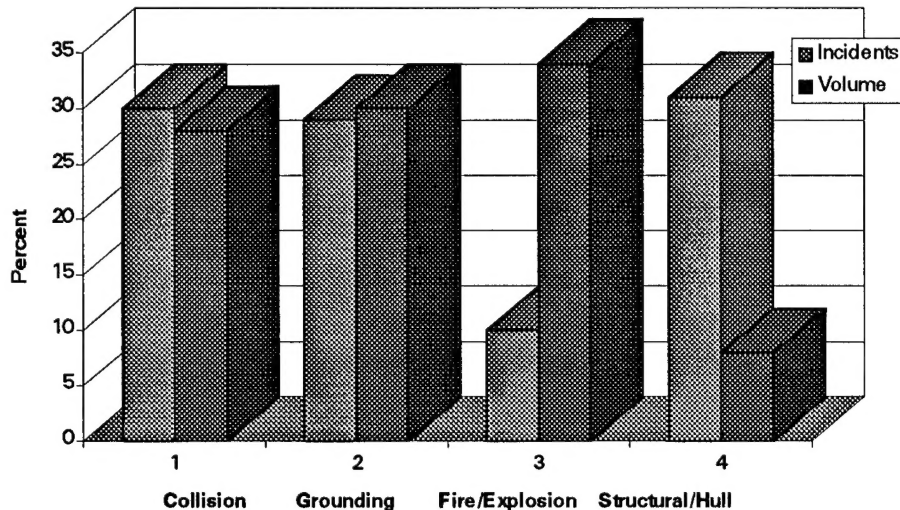


Figure 1 - 2: Major Tanker Oil Spills and Causes

The maritime industry has been identified as a high risk operation, requiring an active risk management program.<sup>2</sup> The U.S. Coast Guard (USCG) has expressed a commitment to reduce the risks of the maritime industry. There have been a number of major tanker owners who have expressed the same commitment of cooperation with the USCG [8]. Rear Admiral Card (Chief, Office of Marine Safety, Security, and Environmental Protection, USCG), has entrusted both industry and the USCG to make "prevention a strategic concept."<sup>3</sup> Yet, to effect the appropriate risk management program, there must be an appreciation for the risk at hand.

While the possibility of an oil spill provides the impetus to investigate groundings, it must be remembered that the magnitude of oil outflow is a function of many unpredictable cir-

<sup>2</sup> Based on roundtable discussion at the High Consequence Operations Safety Symposium, Sandia National Laboratories, Albuquerque, New Mexico, July 1984. Other industries identified include: nuclear power generation; nuclear weapons assembly, storage, and disassembly; commercial aviation; chemical and petroleum processing.

<sup>3</sup> Card, J.C. Speech, Training and the Human Element in Accident Prevention Conference, The Center for Maritime Education, Seamen's Church Institute of New York and New Jersey, October, 11 1995.

cumstances. There can be groundings that are preceded by marked and profound blunders, yet, the degree of oil spilled may be negligible. So while limiting oil outflow motivates the investigation of groundings, the scope is much broader and concerns itself with the nature of the events leading to the vessel's grounding. Hence, the ultimate goal is to understand the nature of the errors that lead to a grounding. Once understood, the proper policy and technology can be implemented to reduce groundings and serve to make the maritime industry safer in all respects.

## 1.2 The Approach

To understand the mechanisms that lead to a tanker grounding, there must be a systematic approach. Probabilistic risk assessment (PRA) techniques provide a systematic process to follow that can give a better understanding of the accident mechanisms that lead to a tanker grounding.

The PRA provides a formal process of determining the full range of possible adverse occurrences, probabilities, and expected costs for any undesirable event. It is a technique for identifying, characterizing, quantifying, and evaluating hazards [33]. Additionally, it can identify those areas that offer the greatest risk-reducing potential. Once the components with the greatest risk-reducing potential are identified, appropriate technology and management schemes can be developed to properly influence risk reduction.

Figure 1-3 shows a proposed risk model fore the tanker industry [1]. This model outlines three levels of assessment for developing an overall risk assessment.

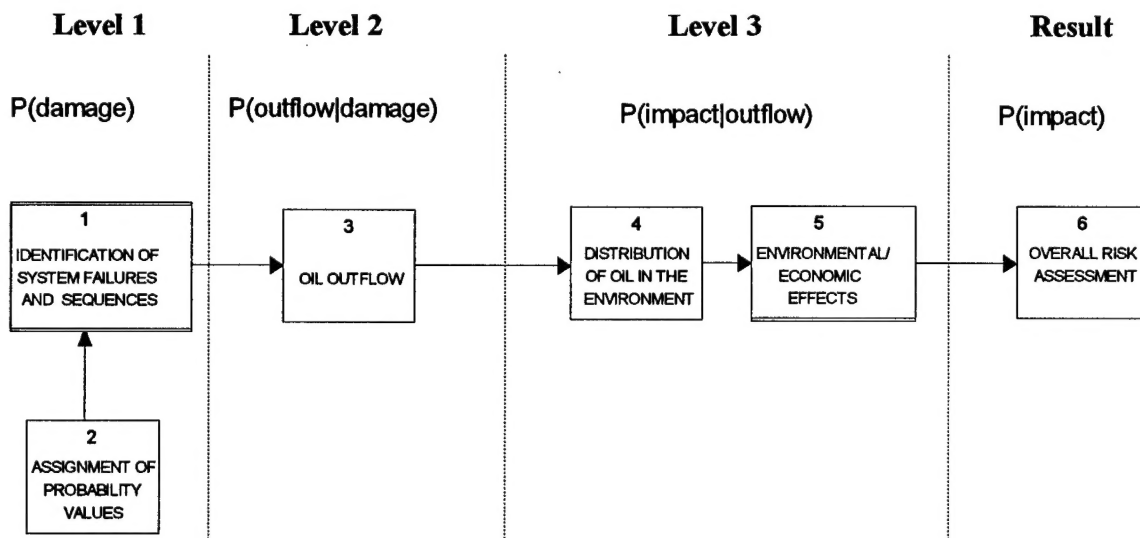


Figure 1 - 3: Risk Model

**Level 1:** Develop a probability of damage and the extent to the ship as the it responds to an initiating event:  $P(\text{damage extent})$ .

**Level 2:** Given that an extent of damage has occurred, what is the probability that oil will outflow to the environment:  $P(\text{outflow}|\text{damage extent})$ .

**Level 3:** Given that oil is released to the environment, what is the probability of consequences to the environment:  $P(\text{impact}|\text{outflow})$ .

**Result:** The probability of oil pollution producing adverse economic and environmental consequences:

$$P(\text{impact}) = P(\text{damage extent}) \times P(\text{outflow}|\text{damage extent}) \times P(\text{impact}|\text{outflow})$$

Previous work has concentrated on the grounding problem, specifically, identifying the system failures in level 1 [1]. This thesis will concentrate on the level 1 analysis for groundings by identifying the error sequences and identifying the error probabilities to determine the probability of grounding for a tanker.

### 1.3 Discussion

Many accident studies have been limited to the place where the accident occurred and limited to a small period of time preceding the accident [20]. The results have typically been interpreted as some form of carelessness on behalf of the individuals [52]. Traditional reactions to maritime accidents, which have been labeled as being primarily caused by human error, have led to the study of mariner skills and responses. As a result, punitive measures have been implemented to deter unsafe practices.

The risks involved with the maritime industry, and more specifically, the tanker industry, need to be better understood. Placing blame on the front-line operators and installing a punitive model is short-sighted. There needs to be a systematic approach to understand, identify, and minimize the risks. Once the risks are understood, and consideration is made of all the issues, the components of the system, and their synergism, the proper framework can be developed which addresses a wholesale solution rather than discrete problems.

An understanding of the nature of the risks involved can be an impetus for cultural change throughout the maritime industry--yielding a balanced approach to managing safety performance. The goal is to have safe and profitable operations balanced by the interaction of management, the work environment, human behavior, and technology, all supported on a firm foundation of sound rules, regulations, and standards [8].

The culture, design, and operation of the maritime industry all contribute to create an error-inducing system [42]. While risk acceptance and risky behavior are often attributed to the "traditions of the sea" [42], the risks associated with sea transportation are no longer restricted to the domain of the seafarer.<sup>4</sup> Accidents such as the *Exxon Valdez*, *Braer*, and the

---

<sup>4</sup> The etymology of risk offers some insight. Derived from the Latin, *risicum*, it is the challenge presented by a barrier reef to a sailor.

more recent *Sea Empress* groundings have broadened the arena of active involvement. As oil tankers have gotten larger, the tolerance for error has decreased as the consequences have increased. However, society's concerns are not as much about the proportionate increase in tanker size, as the disproportionate increase in the potential environmental impact [52]. While the tanker industry has been identified by the USCG as a high-risk industry, the USCG has also stated that the industry has a high potential for improvement [8].

The nature, magnitude, and importance of the risks and associated consequences of sea transportation of petroleum products requires a common knowledge of all the concerned parties. Hence, a systematic approach must be undertaken to effectively communicate the risks and consequences so that they can be minimized by the appropriate safety measures. The PRA offers that total systems approach

## 1.4 Outline

Chapter 2 presents an evaluation of the nature of oil spills, the grounding problem and the associated difficulties of existing databases. Chapter 3 presents the level 1 risk assessment methodology to be utilized. Since the human contribution to failure is significant, a review of contemporary human failure theory is necessary to understand the underlying implications of human behavior and cognitive engineering on the performance of tankers. Chapter 4 looks at the theory of human failure analysis. Chapter 5 then outlines the methodology required to quantify the human related failure probabilities. Chapter 6 provides the rationale for the failure sequence development and assigns probabilities to determine the probability of grounding. In conclusion, chapter 7 evaluates the results and offers some recommendations.



## Chapter 2 The Nature of the Problem

### 2.1 The Tanker Problem

The international sea trade, and the tanker industry in particular, have been operating in a volatile market since the global recession of the 1980's. The tanker industry is prone to oversupply [57]. The seemingly erratic nature of freight rates and the potential for large capital appreciation when the freight rates soar, provides an inherent optimism within the industry. The availability of financing and government subsidies minimize barriers into the industry and fuel optimism. The tanker market has been described as being close to a perfectly competitive market [57]. However, the market is highly fragmented, as such, shipping companies do not exercise pricing power and they tend to accept whatever freight rates the market will bear--even below the break-even point [57]. Therefore, readily available financing and over optimism keeps an over supply of tankers competing for below cost freight rates providing an impetus to the ship owner to reduce costs where ever possible. As a result, open registry countries continue to attract a major portion of the tanker fleet. By registering a vessel under a "flag of convenience" (FOC), shipowners are able to incur the benefits of tax allowances, the freedom to crew ships with low-wage labor, and often, less stringent vessel classification and inspection rules [43].

The principal countries offering flags of convenience are summarized in Table 2-1. These five FOCs represent nearly 40 percent of the world's tanker tonnage [63].

**Table 2 - 1: Registered Tonnage (vessels greater than 1000 dwt) in Principal FOCs  
(Status: December 31, 1993)**

Country	Tanker Tonnage (1000 dwt)	Total Tonnage (1000 dwt)	Share of Tonnage Owned by Nationals in the Total Register Fleet (%)
Liberia	49,030	88,354	0.0
Panama	32,857	82,992	0.0
Cyprus	6,168	32,669	8.4
Bahamas	17,913	33,062	0.4
Bermuda	3,755	5,098	0.0

According to the UK P&I club, Panama and Cyprus stand out for having a significant number of claims for structural failures compared to the number of ships registered under the respective flags [60]. Furthermore, Panama's poor performance as a flag state is indicated by the fact that over a third of the global tonnage lost in 1992 flew the Panamanian flag [25]. Table 2-2 [25] shows the number of vessel losses and the total gross tonnage lost for these FOCs.

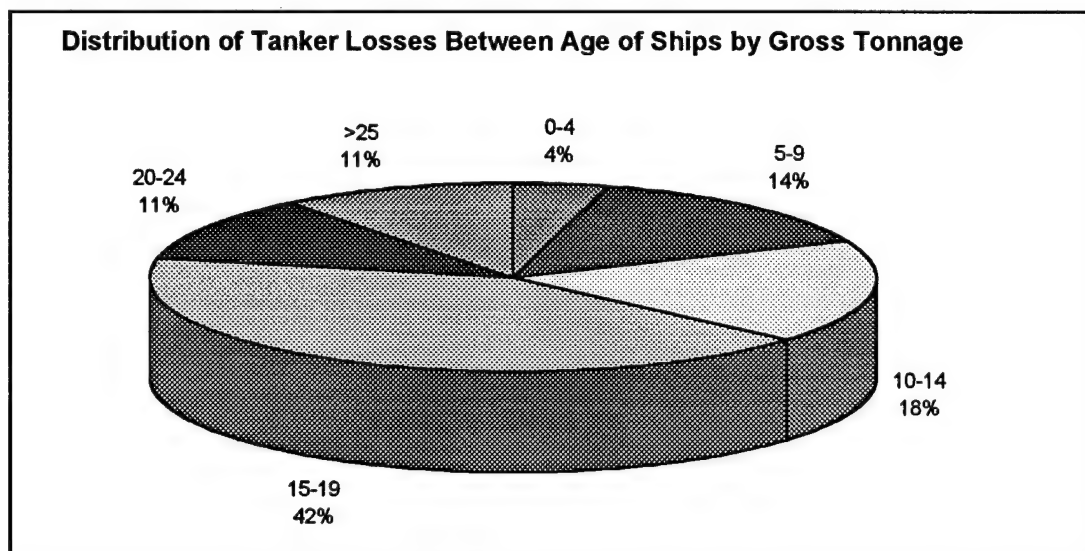
**Table 2 - 2: Number of Losses and Gross Tonnage Lost from 1988 - 1992 (Vessels > 500 gross tons)**

Country	Number of Losses	Gross Tonnage Lost
Panama	135	751,792
Cyprus	50	655,989

Along with the trend of outflagging vessels, there has been a demonstrated change in the way many ships are managed. More shipowners are passing their responsibility for asset marketing and operations to professional ship management organizations. These organizations are typically private companies that are not involved with ownership but engage in managing vessels on a contractual basis to secure the best rate of return on the shipowner's investment [43]. In addition to third party management, mortgage banks are typically involved, having proprietary rights to vessels [43].<sup>5</sup>

As a result of registering vessels under FOCs and utilizing third party management, it is often difficult to determine accountability should a mishap occur.

Another cost-cutting strategy adopted by shipowners is to extend the life of their vessels. Consequently, the age of the tanker fleet is growing. Before 1980, the average age of a tanker to be scrapped was 15 years [43]. In 1993, the average age of the active tanker fleet was 16.9 years [63]. It is expected that the average tanker age will increase by 5 percent per year [43]. While it is difficult to attribute accident causality directly to tanker age, there are some alarming statistics. For example, 99 percent of the tanker losses in 1992 involved ships which were at least 17 years old [25]. Figure 2-1 [25] shows the distribution of tanker losses by age between 1988 and 1992.



**Figure 2 - 1: Distribution of Tanker Losses by Years of Age by Gross Tonnage (1988 - 1992)**

<sup>5</sup> The whole issue is exacerbated by subsidies to encourage shipbuilding, banks willing to lend based on government guarantees, and shipowners willing to gamble on the next big boon. The result is an over-tonnage of vessels and consequential bankruptcies.

Those tankers greater than 15 years old represent 64 percent of all tanker losses by gross tonnage.

The trend for older tankers to represent a greater proportion of all losses has been consistent. Figure 2-2 [25] compares the number of tanker losses by age for the years 1982 and 1992.

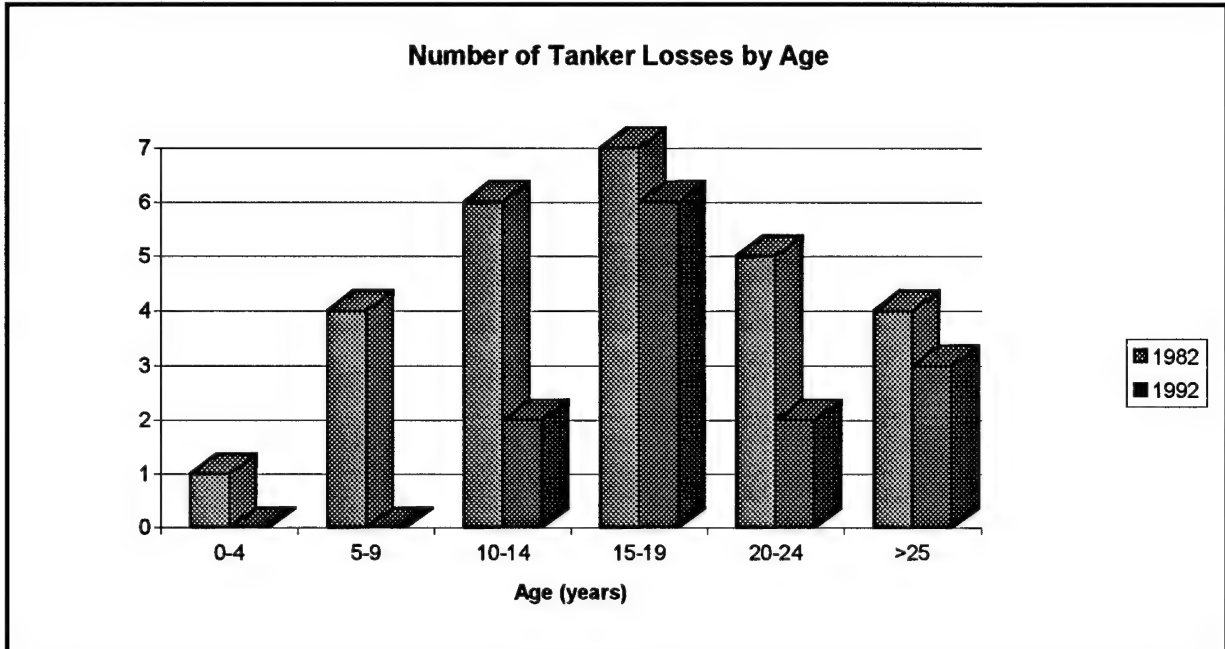


Figure 2 - 2: Number of Tanker Losses by Age ( 1982 and 1992)

Claims against the UK P&I Club for structural or pollution damage tend to give the same distribution with age [60].

Ship structures deteriorate with time and the deterioration accelerates in the absence of proper maintenance. If maintenance expenditures are reduced and maintenance intervals extended to further cut costs, then accident intervals will increase. Commercial pressures have induced masters to exceed reasonable loading practices and to operate ships beyond design limits.

Many vessels are manned by low-wage personnel from developing countries. Often these crews are not qualified. It is not unreasonable to find a 20 year old tanker registered under a FOC, with third party management, classed by a less than scrupulous classification society, implementing poor maintenance procedures done by unqualified low-wage personnel and supervised by officers speaking a different language from the crew.

There are attempts to impede the unscrupulous ship owner. The International Association of Classification Societies (IACS), has been formed to consolidate the group of reputable classification societies. Port State controls have been implemented to help identify sub-standard tankers. Yet, there still exists a large contingency of sub-standard vessels.

## 2.2 Oil Spill Data

The International Tanker Owners Pollution Federation maintains a database of oil spills from tankers, combined carriers, and barges. Data is based on spills over 7 metric tons. Estimates of the amount of oil spilled into the marine environment for each year between 1970 and 1994 are shown in Figure 2-3 [I2].

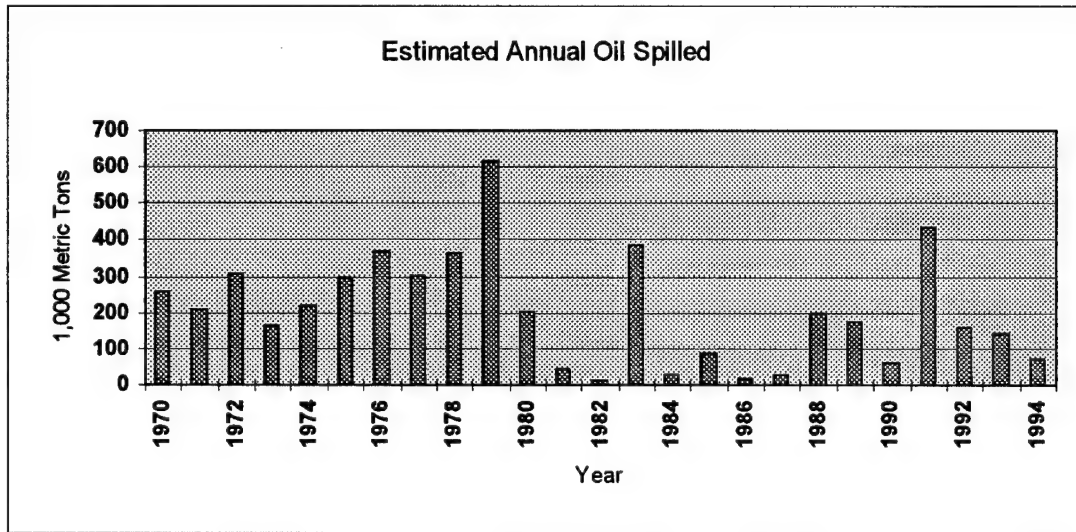


Figure 2 - 3: Estimated Annual World Wide Oil Spilled

Most spills however, are small, and international data for small spills is either incomplete or unreliable. It has been suggested that the contribution of small spills to the total amount of oil entering the oceans from the tanker industry is small. However, a review of the domestic data tells a different story. The USCG's data base tracks spills in U.S. waters and spills abroad from U.S. flagged ships. The distribution of oil spills from major (> 10,000 gallons), medium (1,000 - 10,000 gallons), and small (<1,000 gallons) spills is shown in Figure 2-4.<sup>6</sup> Small spills represent anywhere from 4 to 32 percent of the total volume spilled.

While the distribution shows that the medium and small spills have varied significantly as a percentage of total amount spilled, Figure 2-5 shows that the volume of oil from small spills has remained relatively constant.

It may be argued that major spills have been reduced in recent years; however, data suggests that the volume of spills from small and medium spills have remained relatively constant. The data from the USCG suggests that small and medium spills represent a significant percentage of the total volume spilled. In fact, since 1991, the USCG's database shows that small and medium spills account for more oil pollution than large spills.

<sup>6</sup> One metric ton equals 2,205 pounds, or 7.33 barrels, or 308 gallons (based on average Arabian Light 33.5o API gravity).

In summary, it remains a difficult task to estimate worldwide spill volumes. Globally, data for spills is collected only for large spills. Yet, in the U.S. small and medium spills offer a significant contribution. It could be conjectured that this pattern is applicable on a global scale.

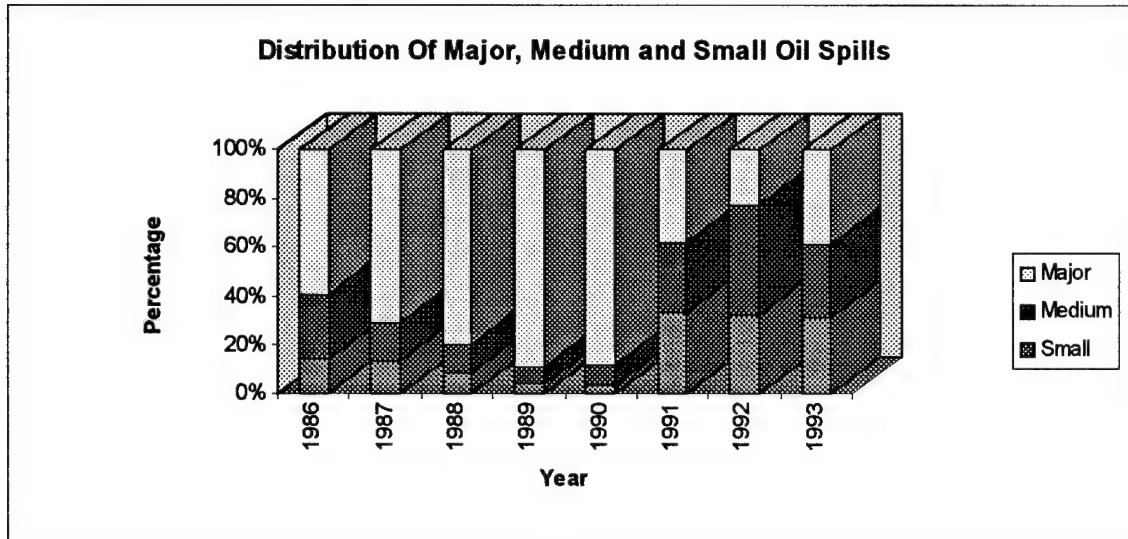


Figure 2 - 4: Distribution of Spills in U.S. Waters and U.S. Flagged Vessels

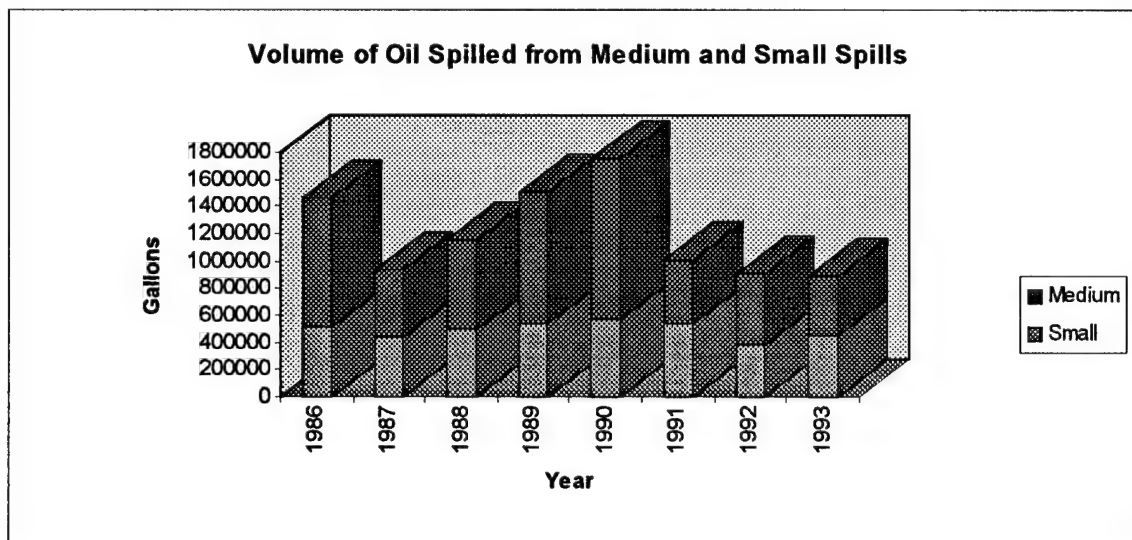


Figure 2 - 5: Volume of Oil Spilled from Major and Small Spills in U.S. Waters and by U.S. Flagged Vessels

Given the difficulty in determining spill volumes, it is just as difficult to determine any absolutes from trend analysis of the oil spill statistics. Peaks in Figure 2-3 are dominated by a few very large spills. Table 2-3 [I2] shows the volume from a selection of major oil spills.

**Table 2 - 3: Selected Major Oil Spills**

<b>Year</b>	<b>Vessel</b>	<b>Volume Spilled (millions of gallons)</b>
1979	<i>Atlantic Empress</i>	86
1983	<i>Castillo de Bellver</i>	79
1991	<i>ABT Summer</i>	80

Nearly half of the total spill volume in 1994 is a result of the *Braer*. Furthermore, since 1985, 10 spills account for 74 percent of all the major spill incidents by volume [12].

Highly visible oil spills have made society more aware of the potential dangers inherent with transporting oil at sea. Yet, the general public is oblivious to many significant spills. Table 2-4 lists the five largest spills world-wide for years 1993 and 1994.

**Table 2 - 4: Five Largest Tanker Spills 1993-1994**

<b>Date</b>	<b>Vessel</b>	<b>Spill Volume (millions of gallons)</b>	<b>Location</b>
1/5/93	<i>Braer</i>	25	Shetland Islands, Scotland
10/21/94	<i>Thanassis A.</i>	11	South China Sea, 400 mi off Hong Kong
3/13/94	<i>Nassia</i>	9	Entrance to Bosphorus Strait, Turkey
1/20/93	<i>Maersk Navigator</i>	7	Strait of Malacca, Singapore
1/24/94	<i>Cosmas A</i>	7	South China Sea, 300 mi off Hong Kong

While many of these spills have escaped scrutiny by society at large, they represent a significant potential threat to the marine environment.

Major spills seem to occur erratically. The clustering of events in a randomly generated sequence of events is expected. A sequence of events in the U.S., initiated by the *Exxon Valdez*, led to the Oil Pollution Act of 1990 (OPA 90). While spills in U.S. waters have decreased significantly since implementing this legislation, the question remains: Has OPA 90 been effective in reducing oil spills? "One of the problems with randomly occurring processes is, that measures, whatever they are, are sometimes seen to be effective" [20]. The fundamental question to be asked is: "How much of the process is random and how much is systematic" [20]? Until there is a better understanding of the accident mechanisms, any attempts to minimize their occurrences are reactionary with questionable effectiveness.

## 2.3 Summary

Oil tankers represent 38 percent of the world's fleet by tonnage [63].<sup>7</sup> Nearly half of all the seaborne trade is involved with the transportation of crude oil and other petroleum products [63]. Figure 2-6 [63] shows the distribution of seaborne trade between the primary cargoes. The distribution of cargoes that comprise this trade is telling, in terms of the nature of the risk of an oil spill [52].

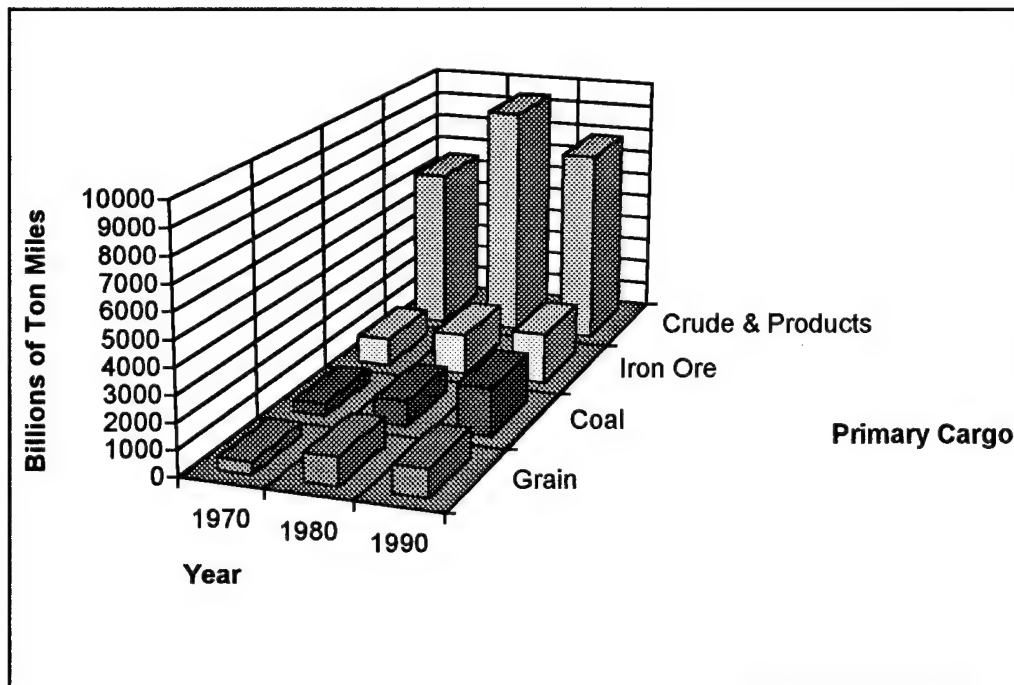


Figure 2 - 6: World Seaborne Trade by Types of Cargo

It is difficult to estimate the total amount of petroleum hydrocarbons entering the world's oceans. However, tanker spills appear to represent a significant contribution of all of the petroleum hydrocarbons introduced into the marine environment. Even though estimates show that the contribution has decreased by nearly 70 percent, it is difficult to determine if the trend is from initiatives implemented by tanker owners, oil companies and regulatory bodies. The erratic nature of major accidents implies a randomness, and the clustering of random events is expected. To be able to understand the data, there must be a fundamental understanding of the accident mechanisms which result in oil spills. The nature of oil spills can be

<sup>7</sup> At the end of 1993, the oil tanker fleet represented 271,222,000 dwt, 38.2 percent of the world's fleet by dwt [63].

better understood through a systematic analysis. Only then can the systematic causes be filtered from the apparent randomness and properly addressed.

Certain FOCs have a demonstrated poor accident performance. The fact of an owner choosing a particular flag does not give any reason to assume that the owner is seeking to lower his own standards through using a flag of poor performance. However, an owner who is not fully committed to quality is likely to be attracted by such flags [60].

The NRC found that for tankers over 10,000 dwt, grounding events dominate in terms of both numbers of accidents and the volume spilled [36]. It can be inferred that the primary reason for a grounding is an improper human response to an indication [1]. In essence, human failures prevail as the predominate factors in grounding accidents. Human error has consistently been attributed to 80 percent of marine casualties [38]. To be able to identify and quantify the human related errors involved with the groundings, there must be a thorough understanding of human reliability and human factors to minimize the myopic condemnation of front-line operators.



## **Chapter 3 Risk Assessment**

### **3.1 The Probabilistic Risk Assessment**

Marine transportation operations are high risk and require an active risk management program. Even though the ratio of oil spilled to oil transported is extremely small, there is plenty of room for improvement. Hence, there is a need for a systematic approach to determine the risks involved with transporting oil at sea. What is more important, is the need to determine the risk reducing potential. By identifying those areas with high potential for reduction, limited economic resources can be utilized more effectively. There is momentum in the industry for change, and the outlined systematic approach offered by a PRA yields the areas of change to which the industry can focus.

The PRA is a natural tool to assist in risk management decision making to prevent oil spills [55]. It provides a formal process of determining the full range of possible adverse occurrences, probabilities, and expected costs for any undesirable event. The PRA is a technique for identifying, characterizing, quantifying, and evaluating hazards [33]. In addition, it can identify those areas that offer the greatest risk-reducing potential. Once the components with the greatest risk-reducing potential are identified, appropriate technology and management schemes can properly influence risk reduction.

The approach to be undertaken has matured in the nuclear industry. The nuclear industry has committed a great deal of time and effort in the study of cognitive engineering to minimize the probability of high consequence accidents. Many of the issues undertaken in the nuclear industry are germane to the oil tanker industry. Nuclear power stations and oil tankers generate public anxieties when operated close to population centers and they are targets of environmental lobbies in the aftermath of an accident [53]. Additionally, both operate in an environment where it is often difficult to quantitatively ascertain the effects that all the influencing variables have on operational safety [53]. Given the similarities, it is the intent of this project to take the risk assessment methodology that is firmly established in the nuclear industry and apply it to the maritime industry.

The proposed risk model (Figure 1-3) outlines three levels of assessment that will lead to the ultimate probability of oil pollution producing an impact. This thesis will concentrate on one aspect of a level 1 analysis--tanker groundings.

The approach has its foundations in the risk model and the event tree/fault tree methodology. The event tree/fault tree approach employs discrete logic diagrams to explicitly show the causal relationships within the system model to determine the probability of the accident scenarios. The methodology is widely used in technological systems applications [55], but it is also routinely performed to determine human reliability [17]. Since humans have been directly attributed to over 80 percent of maritime casualties [38], it seems important to utilize a method that is consistent with both the technical and the human aspects of the system.

## 3.2 Fault Trees

Complex systems that have multiple failure modes with physical and operational interactions lend themselves to fault tree analysis, especially if the role of humans in the operation needs to be modeled [33].

A fault tree is a graphical display to show how basic component failures can lead to a pre-determined system failure state. In constructing a fault tree, one starts with a particular failure or undesired event and deductively works backwards to explore all the combinations of events that may lead to that particular failure. The reasoning used to build a fault tree for a system requires an understanding of the system and its intended use. At each reduction stage of the fault tree, the general causes for the undesirable top event must be determined in as broad of terms as possible. By being as general as possible at each reduction stage, it is more likely that all possible combinations of events may be taken into account. "Elegant simplicity instead of unnecessary complexity is to be encouraged" [3].

A minimum cut set is defined as a minimal set of system components such that if all the components fail, system failure results, but if any one component has not failed, no system failure results [44]. Once the system is depicted in a logic diagram, the minimum cut sets can be determined. When the minimum cut sets are identified, the appropriate probabilities can be assigned and the probability of the top event can be calculated.

The fundamental building blocks of fault trees are the AND-gate and the OR-gate (Figure 3-1).

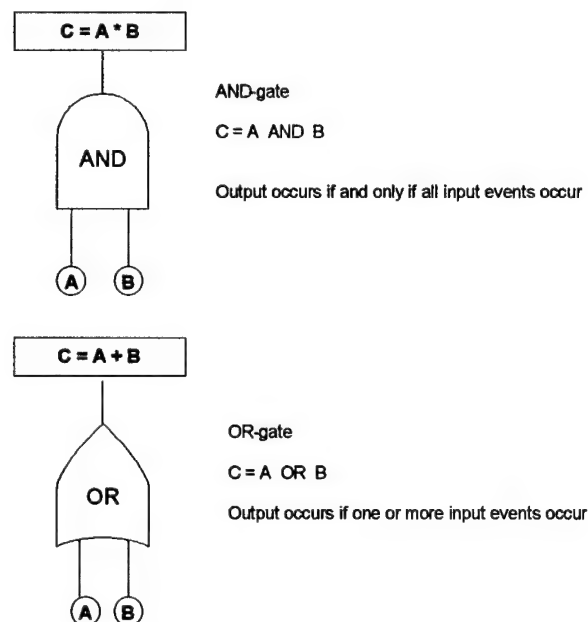
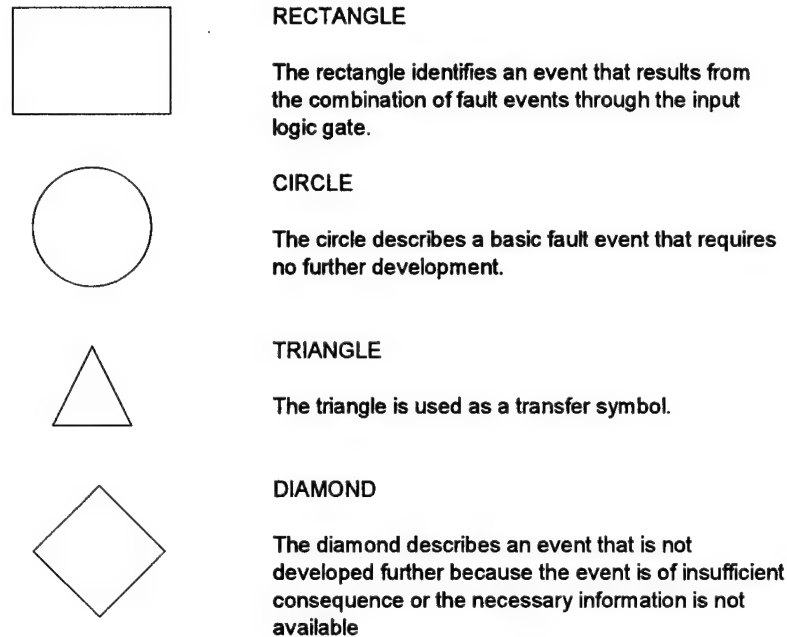


Figure 3 - 1: AND-gate and OR-gate

An AND operation requires that all the input faults occur for the output fault to occur. The AND operation corresponds to the intersection operation in set theory. An OR operation

requires that only one input fault occur for the output fault to occur. The OR operation corresponds to the union operation in set theory. Additional notation used for fault trees are described in Figure 3-2.



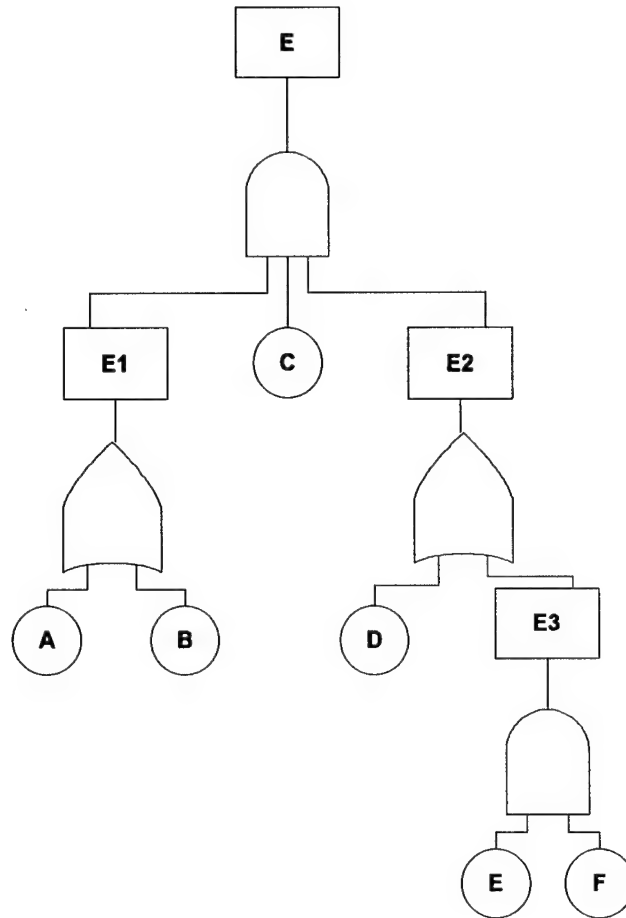
**Figure 3 - 2: Fault Tree Symbolism**

### **3.2.1 Fault Tree Evaluation**

The fault tree, although qualitative in nature, provides the framework for a quantitative evaluation [45]. Evaluation of a fault tree typically involves a top-down successive substitution process invoking Boolean identities. The goal is to represent the fault tree by a reduced form Boolean expression. The reduced expression then represents the minimal cut sets.

Consider the fault tree in Figure 3-3. For the top event E, there are:

- Three intermediate events: E1, E2, and E3.
- Six basic events: A, B, C, D, E, and F.



**Figure 3 - 3: Example Fault Tree**

The expression for the top event E, is given by:

$$\begin{aligned}
 E &= (E1 * C * E2) \\
 &= (A + B) * C * (D + E3) \\
 &= (A + B) * C * (D + (E * F))
 \end{aligned}
 \tag{3-1}$$

If all the basic events are independent of each other, then the probability of the top event E is given as:

$$P(E) = [P(A) + P(B) - P(A * B)] * [P(C)] * [P(D) + P(E * F) - P(D * E * F)]
 \tag{3-2}$$

Basic properties, rules of probability and Boolean identities are provided in Appendix A.

There are limitations to the fault tree approach that must be recognized. Primarily, the limitations involve the completeness, the adequacy of the data, and the binary nature of the fault tree. Any quantification of the fault tree is constrained by these areas [45].

### 3.3 Event Trees

Event trees are used to display the results of a task analysis. The complete event-space, consisting of possible events in a system is represented pictorially. The tasks are made up of fundamental events. As the event is carried out, it is completed either successfully or unsuccessfully. Each limb of the tree represents a binary process and is annotated with the probability of success or failure. Refer to Figure 3-4. As the event tree progresses from left to right, each event is considered in a binary state, that is, it either succeeds or fails. Each success limb moves up, while each failure limb moves down. Recall that the basic properties and rules of probability are provided in Appendix A.

#### 3.3.1 Event Tree Evaluation

For some initiating event A (Figure 3-4), there is a corresponding probability of successful completion or failure:

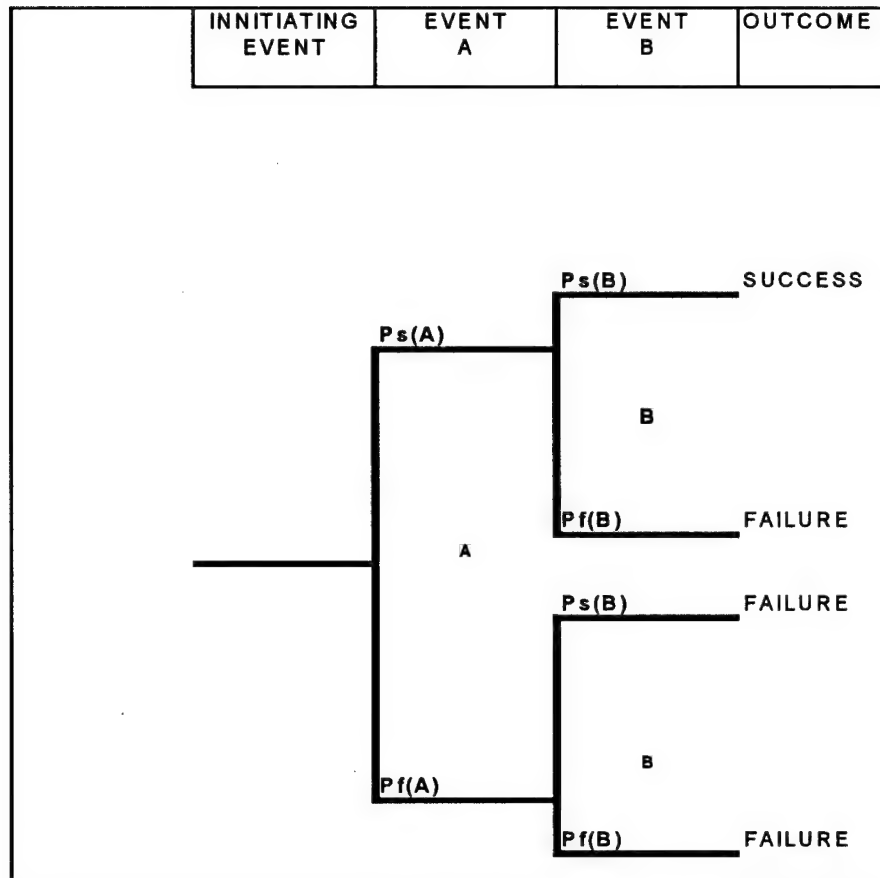
$$Ps(A) = \text{probability of successful performance of task A} \quad (3-3)$$

$$Pf(A) = \text{probability of unsuccessful performance of task A} \quad (3-4)$$

Given the two outcomes of event A, event B can then either be performed successfully or unsuccessfully:

$$Ps(B) = \text{probability of successful completion of event B} \quad (3-5)$$

$$Pf(B) = \text{probability of unsuccessful completion of event B} \quad (3-6)$$



**Figure 3 - 4: Event Tree Diagram**

The probability of successfully completing this task is then computed by multiplying the probabilities of occurrence of each of the events that constitutes the success path:<sup>8</sup>

$$\begin{aligned}
 P(S) &= \text{the probability of successful completion of the task} \\
 &= P_s(A) * P_s(B)
 \end{aligned}
 \tag{3-7}$$

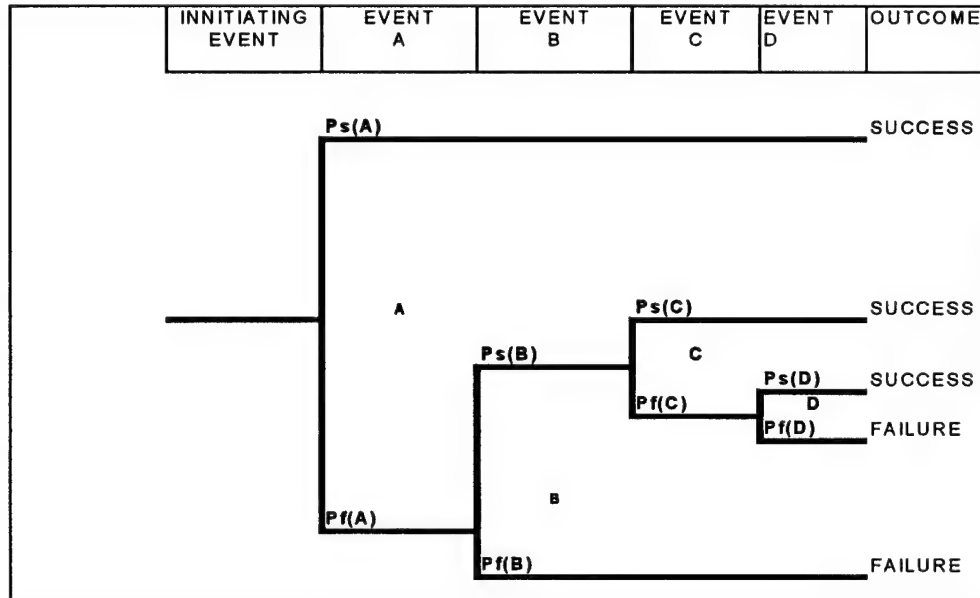
$$\begin{aligned}
 P(F) &= \text{the probability of unsuccessful completion of the task} \\
 &= 1 - P(S)
 \end{aligned}
 \tag{3-8}$$

This use of event trees to model performance reliability assumes that each path is mutually exclusive and the system can be modeled with sequential logic.

The use of event trees can become unwieldy as the number of events increases. For  $n$  events, there are  $2^n$  possible paths. To reduce the number of paths, the events can be deduced such that irrespective of subsequent events, success or failure remains constant. Consider a four event system consisting of events A, B, C and D. For this system, if event A is successful, then regardless of events B, C, and D, the system will succeed. Similarly, if event B is unsuccessful, then regardless of events C and D, the system will fail. Following this line of reason-

<sup>8</sup> It must be emphasized that this method assumes that the event probabilities are independent.

ing, where the outcome of subsequent events is inconsequential to the state of the system, then that leg need not be further developed. The event tree can be reduced to five paths instead of 16. Refer to Figure 3-5.



**Figure 3 - 5: Reduced Event Tree**

For the system in Figure 3-5, system reliability can be calculated as follows:

$$P(S) = P_s(A) + (P_f(A) * P_s(B) * P_s(C)) + (P_f(A) * P_s(B) * P_f(C) * P_s(D)) \quad (3-9)$$

$$P(F) = (P_f(A) * P_s(B) * P_f(C) * P_f(D)) + (P_f(A) * P_f(B)) \quad (3-10)$$

$$P(S) = 1 - P(F) \quad (3-11)$$

### 3.4 The Grounding Fault Tree

A fault tree for tanker groundings has been previously developed (Figure 3-6) [1]. By expounding on these concepts, the fault tree will be verified and those fundamental items of the fault tree will be further investigated. Event trees will be developed to assist in assigning probability values. Appendix B is provided to give the rationale used in developing the grounding fault tree.





### 3.5 Summary

The maritime culture, economics, and regulatory bodies all contribute to create a system that can be characterized as error-inducing. There has been little effort to characterize the system as a whole and to determine the areas that offer the greatest potential for risk reduction. The NRC has determined that maritime safety as a whole, could benefit from the increased use of quantitative and qualitative risk analysis to develop risk reduction strategies [35].

The outlined approach has its foundations in the risk model and the event tree/fault tree methodology. Siu *et al.* [55], have argued that the event tree/fault tree approach provides a natural framework for treating oil spill scenarios.

When developing a PRA for oil spills it is important to recognize the areas of uncertainty. The PRA is a discrete analysis. Therefore, it is unable to account for the infinite number of possibilities. Ideally, a PRA considers all the important aspects that lead to the undesired event, but there is the possibility that important contributions have been overlooked. Additionally, there are uncertainties due to the necessary approximations made in developing the model. Human failure factors, system complexity, and the subjective nature of the analysis, all present uncertainties that must be recognized. Despite the uncertainties, it is important to develop a PRA so that perceived risk does not produce either irrational behavior or reflex reactions. The performance of a PRA reduces the uncertainty concerning some of the elements of risk so that resources can be better allocated.

The performance of a risk analysis of and by itself can reduce risk as knowledge and awareness are gained [12]. Additionally, if the process of risk assessment is dynamic, the uncertainties can diminish with time as more knowledge is gained. Once the PRA is completed, allocating resources in the areas that are risk relevant, rather than trying to alleviate all conceivable hazards, allows for realizable risk reductions with limited resources.

## **Chapter 4 The Human Problem**

### **4.1 The Importance of the Human Problem**

The first step of a PRA is to identify system failures and sequences. The fault tree for tanker groundings was developed to determine the basic failures. The bottom layer of the fault tree describes the fundamental causes for tanker groundings. Qualitatively, human failure and individual error are significant in the progression of events leading to a tanker grounding. Therefore, to minimize the probability of failure, the human contribution must play an integral role in the PRA.

### **4.1 The Historical Pervasiveness**

The failure of humans has long been recognized to have a substantial impact on the reliability of complex systems [33]. The pervasiveness of human failure in the maritime industry has been recognized for a number of years. Human failure is a problem that must be addressed to effect any changes to the system.

In 1972, the chairman of the American Hull Insurance Syndicate revealed that 85 percent of the Syndicate's claims payments were for human-error casualties [38]. In 1976, the National Research Council (NRC) attributed 80 percent of vessel collisions, rammings and groundings to human error [38]. More recently, in 1993, the UK P&I Club reported that 62 percent of the major claims associated with commercial shipping were a result of human error [30]. The large number of incidents attributable to human error is not constrained to the commercial arena. A report by the Naval Safety Center found that human error caused 70 to 85 percent of mishaps involving U.S. naval vessels from 1989 to 1993 [32].

The tendency to classify all human errors as individual errors has led to the notion that those particular failures are a part of human nature. Consequently it seems that the high percentage of accidents attributed to human error have become accepted as a norm of the maritime industry.

Casualties are as undesirable to the mariner as they are to the communities that they serve. It is myopic to believe that causality is restricted to those serving on board ships. Yet, it is the front-line operators that are typically blamed. Remember that the ship serves as the mariner's shelter from the environment. It is also the mariner who suffers the immediate consequences of any ill-fated accident. As Singh states [52]:

The least generous interpretation that one is forced to make is that if those on board put into danger, the very receptacle that shelters their lives and personal effects, then it could only be because they had no better response within their repertoire of skills and responses at the time.

In general, the industry maintains a punitive model aimed at those aboard ship with the expectation that accidents will be minimized. However, the scope of causality encompasses a much broader set than that of the front-line operators. The failure of the repertoire provides the reason for research not reproach.

### 4.3 Human Failure and Individual Error

Before delving into the nature of accidents, it is necessary to define an accident. An accident is an event or occurrence that has negative results, effects, or consequences. Accidents can be induced by factors internal and external to the system. Internal factors that cause accidents are system failures. A system failure is an event or occurrence that has negative consequences upon the system's functioning [12].

The problem with the previously cited statistics is the attribution to "human error" and the subsequent interpretation of that term. The term "human error" has been used extensively to attribute causality of some **system failure** to a particular individual. However, "human error," as it is commonly used, encompasses more than just the substandard act of an individual or individuals.

In fact, the term "human error" is unwarranted in many high-risk accidents and its use is a pejoration of the context. It points more to the action as an independent clause, rather than the context in which the action takes place [22]. Hence, it can lead to the mis-allocation of resources and an inability to avoid future accidents. Even though some failures are attributable to people, and it is common to call all such failures human errors, it is the design of the system itself that is prone to error.

Reason [46] distinguishes the human contribution to system failures into two types of errors.

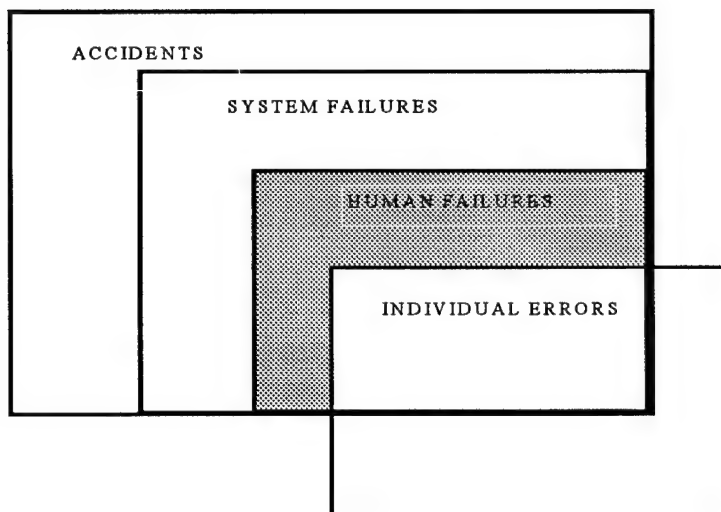
1. *Active errors.* Errors whose effects are felt almost immediately.
2. *Latent errors.* Errors whose adverse consequences may lie dormant within the system for a long time and only become evident when they combine with other factors to breach the system's defenses.

Therefore, human error embraces a far wider range of individuals and activities than those associated with the front-line operation of a system [46]. To incorporate this concept, human error should be realized as a system failure, and it should be broken down into two sets:

1. Human Failure.
2. Individual Errors.

Human failure is a system failure that can be proximally attributed to the actions or inactions of one or more people [12]. Individual errors are also system failures,<sup>9</sup> but their root cause can be attributed to a single person. There can be individual errors that do not have significant consequences and are not a part of an accident's causal chain [42].<sup>10</sup>

The concept of human failure as a subset of system failures allows for the integration of latent errors. Front-line operators tend to be the scapegoat in post accident analysis. In reality, they are the inheritors of latent errors created by poor design, incorrect installation, faulty maintenance and bad management decisions [46]. Figure 4-1, adapted from [12], presents the context of human failures and errors.



**Figure 4 - 1: Context of Human Failures and Individual Errors**

Individual errors may not even comprise half of all the human failures [12]. “In an error-inducing system, the tendency to attribute blame to operator error is particularly prominent” [42]. It has been suggested that the 80 percent ‘human error’ attribution to the maritime industry is better represented as follows [42]:

1. *40 percent individual error*: component failures where the operator is the component that failed.
2. *5 to 10 percent system failures*: accidents that are an integral characteristic of the system, the interactive complexity and tight coupling of the maritime system inevitably will produce an accident.

<sup>9</sup> This model does not consider malicious acts of individuals.

<sup>10</sup> Ordering a right full rudder when a left full rudder was intended is not part of an accident's causal chain if the error is made on the open ocean. However, the consequences in a restricted waterway could be severe.

3. *30 to 35 percent human failures*: errors resulting from a complex and tightly coupled system which requires long hours, has misplaced priorities, and skewed incentives.

A detailed study of marine structures, which experienced some failure, indicated that even though the failures could be attributed to the acts of individuals, the dominant causes were organizational; erroneous actions by groups of individuals that influence the direct cause of failure and exacerbate or escalate its development through compounded errors [6].

As long as humans operate ships, there will be individual errors. Studies of the role of human failures in engineered structures have shown that they are inevitable [4], but many human failures can be prevented through the appropriate combination of management and technology.

## 4.4 Accident Investigations

Accident investigations are predominantly directed at causes low in the system hierarchy--the front-line operators [20]. After an accident has happened, people consistently exaggerate what could have been anticipated [15].<sup>11</sup> The path from hindsight to an event is much more predictable than the exercise of foresight [15].

The hindsight effect fails to give the investigator a true understanding of the root causes of the accident. The hindsight effect leads to implicit stop rules that can bias the investigation to the topical professional issue of the day [52]. As Perrow has discussed [42], the maritime industry is an error-inducing system, and there is a prominent tendency to attribute blame to front-line operators in an error-inducing system.

The myopic approach taken by most investigation regimes has led to number of nebulous studies of the human problem. While studies of human factors in maritime safety have addressed myriad subjects, few of the studies have linked their conclusions to the ship accident experience [16].

"Simply knowing how past disasters happened does not, of itself, prevent future ones" [46]. To gain an understanding of accident causation, investigations must extend the range of individuals and organizations that have to be taken into account. The contributions of individuals, often far removed in time and space from the actual accident must be evaluated [20]. Investigators must take the point of view of the operator to inhibit the hindsight effect. By preventing the hindsight effect, the investigator is less likely to introduce bias and invoke stop rules [52]. When the knowledge gained from accident investigations is combined with adequate theories of error production, a body of principles can be assembled, which can apply to the design, construction, and operation phases of the maritime industry that can reduce the occurrence of errors or their damaging consequences [46].

---

<sup>11</sup> Groeneweg has labeled this the "hindsight effect" [20].

## 4.5 The Pathogen Metaphor

Major disasters are rarely caused by any one factor [46]. They arise from the unforeseeable concatenation of several diverse events, each one necessary but singly insufficient [46]. Reason [46] has suggested a pathogen metaphor to emphasize the significance of causal factors present in the system before an accident sequence begins:

All man-made systems contain potentially destructive agencies, like the pathogens within the human body. At any one time, each complex system will have within it a certain number of latent failures, whose effects are not immediately apparent but that can serve both to promote unsafe acts and to weaken its defense mechanisms. For the most part, they are tolerated, detected and corrected, or kept in check by protective measures (the auto-immune system). But every now and again, a set of external circumstances -- called here local triggers -- arises that combines with these resident pathogens in subtle and often unlikely ways to thwart the system's defenses and to bring about its catastrophic breakdown.

Like the etiology of multiple-cause illnesses due to resident pathogens, complex systems breakdown due to resident latent errors. This concept has been applied by Singh in *The Aetiology of Groundings* [52]. The challenge for this framework is to show how latent and active failures combine to produce accidents and to indicate where and how more effective remedial measures might be applied [46].

## 4.6 Accident Causation

There are numerous schemes to characterize and classify human failures and its causality. Human failure may occur in any phase of the design, construction and operation of a complex system [5]. Unsatisfactory performance can be the result of improper design and construction of the system. Figure 4-2 is adapted from Bea [5] to show more explicitly the context of system failures. An accident can occur due to either external forces ("acts of God"), or some system failure. The system failure causality can be manifested in any or all of the design, construction, and operations processes. The elements of human failure in all three phases are influenced by the synergistic and antagonistic effects of:

1. Individuals.
2. Hardware.
3. Organizations.
4. Environment.
5. Procedures.

However, many errors in the design and construction phase are latent, as such, they remain dormant until perturbed in the operations phase by unsuspecting operators.

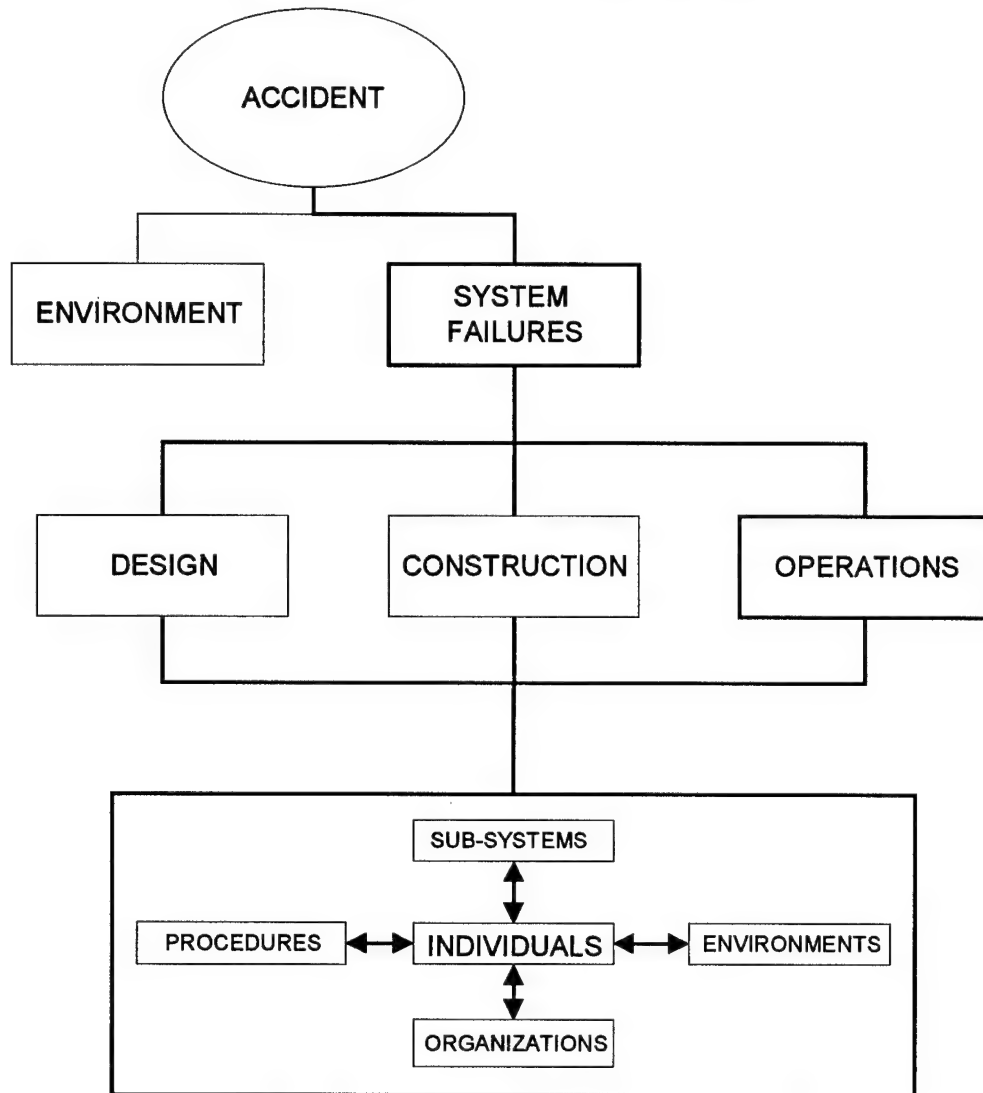


Figure 4 - 2: Human Failure Taxonomy

#### 4.6.1 Design and Construction

Modern vessels are complex systems. The hulls of large vessels must be constructed to withstand the severe forces that the sea imparts. Designers are often motivated to use the least amount of steel rather than build the safest hull. While scantlings are regulated, the design standards are questionable. A study by the NRC [36] found that existing tanker design stan-

dards are no longer adequate. Because of the reduction in design margins, modern tankers are less robust and existing standards must be enhanced.

Hull design is just one aspect of the vessel. The propulsion system, control systems, navigation systems, and communication systems are all a sample of the myriad systems that must be integrated into the hull. With all of these sub-systems of the ship system, design engineers must begin to explicitly evaluate humans as an integral part of the system design to better configure the ship for improved safety [4].

The interfaces between the system and the human must be ergonomically designed to minimize errors. For example, most people can relate to the experience of a learned lecturer having trouble with either a video cassette recorder, slide projector, microphone, etc. The problem is not with the individual, but the design of the system that the individual is trying to use. We have all had problems with doors (pushing instead of pulling), microwave ovens, video cassette recorders, and stereo systems, just to name a few items. Yet there is the tendency to blame either ourselves or the person we are observing as being at fault. In reality, it is the system itself. Norman [40] outlines the following principles of design:

1. *Visibility*. The correct parts must be visible, and they must convey the correct message.
2. *Mappings*. How is what is wanted to be performed perceived from what appears to be possible.
3. *Affordance*. The perceived and actual properties of the system.

Safety features need to be adequately designed into the system to account for possible failures. Recognizing that it is impossible to account for all the possible failures, consideration of the most likely failures with appropriate redundancies can help to reduce catastrophes.

While poor designs propagate through the construction phase, there are additional contributions to accidents that are characteristic of this phase. Failures in the construction phase often relate to the level of quality control and quality assurance. Improper construction materials, inattention, ignorance or the total disregard of design guidelines, and errors in the process of constructing the system are just a sample of the mechanisms for creating latent errors that future operators must deal with.

#### 4.6.2 Operations

Of the three phases, design, construction, and operations, the majority of compromises occur during the operating phase and can be attributed to errors made by operating personnel [5]. Mistakes made during design are compounded during construction and passed to the operators as a complex system that has latent pathogens [46]. Nearly 64 percent of all disasters result from a human failure during operations [34].<sup>12</sup>

---

<sup>12</sup> Moore calls these Human and organizational errors (HOE).



The amount of interdependence reflects the amount of coupling within the system. In a tightly coupled system, each area cannot be addressed in isolation.

#### **4.6.2.1 Sub-Systems**

Sub-systems entail the hardware and software required to support the whole system. Sub-systems of inadequate design exacerbate human failure. The hardware portion of a sub-system is a collection of equipment that has specific intended functions, and interacts among its pieces and with the people and software that operate the sub-system [12]. While technology is increasing equipment reliability, some believe that it is reducing the human reliability of its operation [27]. Engineers are often wont to incorporate new technology, but these new technologies tend to compound latent system flaws [3]. These latent flaws can be manifested in a complex design, close coupling (failure of one component leads to failure of other components), difficult maintenance, and severe performance demands.

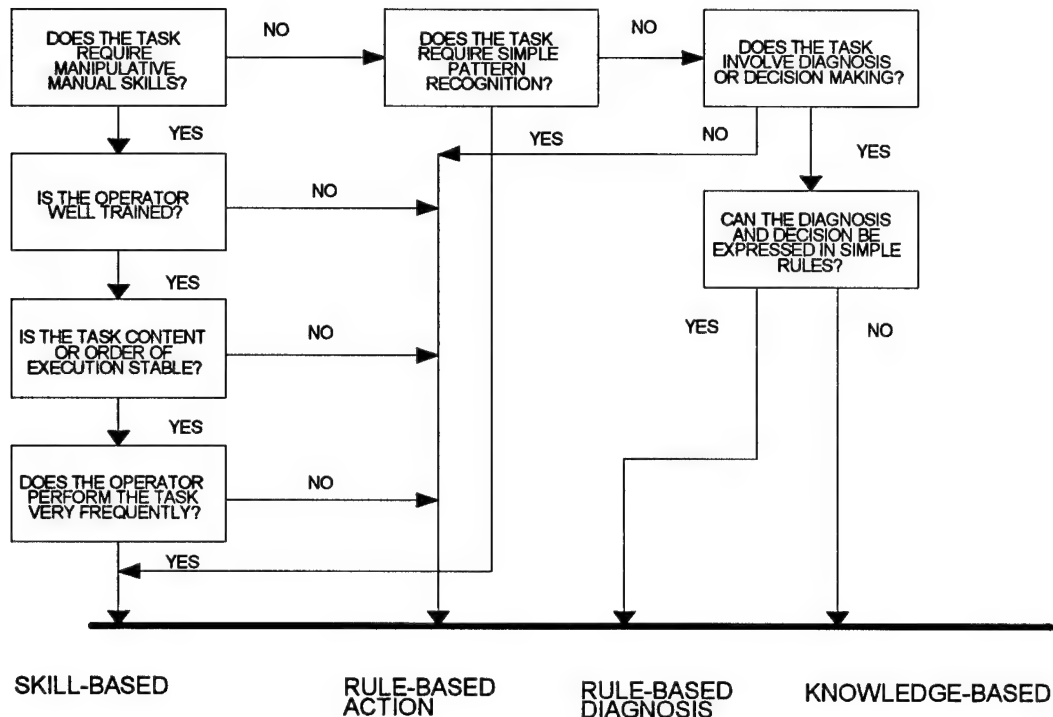
Technology must also balance its ability to liberate human functions with the inevitability of human boredom when operators shift from doing to monitoring. Technological developments incorporating automated systems tend to change the role of the operator from an active to a passive participant. The longer the individual is removed as an active participant, the less likely the person will have a clear understanding of the inner workings of the system should a crisis occur [34].

#### **4.6.2.2 Procedures**

A taxonomic system relating skill, knowledge and rule-based actions to an operational task is shown in Figure 4-3 [12].

The taxonomy shows the role of procedures in terms of a rule-based action and diagnosis based on the complexity of task to be completed. If diagnosis or decision making is needed but no rules are available to assist the activity, then action must be based on a deep fundamental knowledge [12]. Skills include pattern recognition and actions that are manual, well trained, well known, and practiced frequently [12]. Where either skill or knowledge is insufficient or inappropriate, rule based-behavior is essential.

Since absolute skill and knowledge can not be achieved for the various levels of operation of a large vessel, there must be minimum levels of expertise with appropriate procedures. Voyage planning, pre-underway check-off lists and explicit communication procedures are all examples of necessary rules that must come from an overall procedural framework that needs to be developed, evaluated, implemented and enforced.



**Figure 4 - 3: Embrey's Taxonomic System**

#### 4.6.2.3 Organizations

The influence of the organizations on the reliability of marine systems is the most pervasive of the human failure related accidents [3].

Organizations have an impact on individual response as a result of its structure and culture. Both structure and culture are functions of each other. As the NRC states [35]:

The traditional command and leadership relationship has been considered necessary to maintain order and discipline, especially when faced with operating conditions that threaten the vessel, officers, and crew. But the hierarchical structure results in unidirectional, top-down communications. Marine language and practices that derive from this traditional structuring leave little room for the development of a culture that encourages bottom-up communication or the provision of rewards when it happens

... This may be an important deficiency in the marine navigation and piloting system. . . Communication of problems detected by subordinates and solutions they may propose can be stifled by the rigidity of the traditional bridge organization and culture unless the operating company, through the master, has fostered a more receptive bridge team communications environment.

The goals set by an organization can be the impetus for otherwise rational people to make irrational decisions. Pressures to reduce costs and maintain schedules may suppress the prudence of safe operations.

The faulty decisions and subsequent erroneous navigation that leads to an accident can be related to the communication flow-path among the crew. However, it is the organization that establishes the structure of the communication flow-path. The safety of passage requires that the crew function as a team, especially in a restricted maneuvering setting. Sharing information and support among bridge team members is required to safely navigate the range of hazards and conditions encountered [35]. Since access to information is typically divided among the team members, a loss in the smooth functioning of the team results in a break in the flow of information.

Other aspects of the organization that need to be addressed are the individual differences among crew members. These differences are amplified when multi-national crews are employed. Language barriers, cultural and economic background all influence the cohesiveness of the team.

Fundamentally, the faults described above can be broken into two classes of problems facing organizations [3]:

1. *Information*: Who knows what and when.
2. *Incentive*: How are individuals rewarded, what decision criteria do they use, how do these criteria fit the overall objectives of the organization?

#### **4.6.2.4 The Environment**

External and internal environments contribute to individual error.

1. *External factors*: darkness, extreme temperature, storms and other natural phenomena.
2. *Internal factors*: lighting, temperature, noise levels, and vibrations.

Environmental effects can create psychological and physiological human responses that can exacerbate the potential for human failure and individual error.

### **4.7 The Dynamics of Accident Causation**

When one considers all the things that must go wrong for an accident to occur they are truly remarkable events. Within the realm of accidents, system failures have their primary origins in the decisions of designers and high-level managers. At the ship level, the master can exacerbate or mitigate the adverse effects of high level decisions, but the master can also introduce other pathogens into the system. Each of the pathogens introduced into the system can

play a significant role in both provoking and shaping a large set of individual errors. While very few individual errors result in actual damage or injury (giving a wrong rudder order in the open ocean has no effect on the safety of the ship), when errors occur in the presence of some hazard, then the potential for catastrophe is real. System defenses include redundancies, automatic safety devices, and alarms to warn operators of a hazardous situation. Since designers are unable to account for every possible situation, safety systems inherently have windows of opportunity for an accident trajectory to contravene. Circumstantial factors can bias the system to align the mappings of the various failures; creating windows of opportunity through each layer of the system. Accidents occur when the mappings of system failures, human failures and individual errors all conform to allow the accident opportunity to breach each of the layers. Figure 4-4 illustrates the dynamics of an accident.

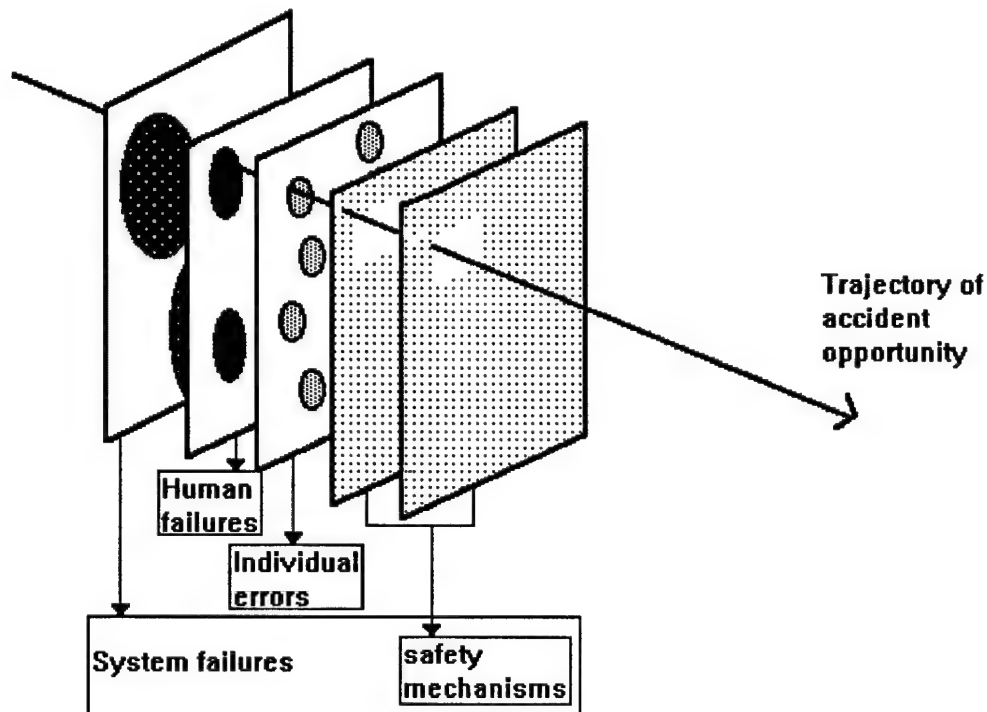


Figure 4 - 4: The Dynamics of Accident Causation

## 4.8 Technology and Risk Homeostasis

The maritime industry has been the recipient of ever improving technologies. The Global Position System (GPS) incorporates satellite technology to allow vessels enhanced navigational accuracy. Microprocessor technology has been incorporated into GPS receivers, Automatic Radar Plotting Aid (ARPA) radars and collision avoidance systems. Laser technology has allowed for massive amounts of information to be stored and read on compact disk

leading to the Electronic Chart Display and Information Systems (ECDIS).<sup>13</sup> Electronic Data Interchange (EDI) incorporates microprocessor, satellite and laser technology. It has the potential to revolutionize the process of data dissemination through the entire shipping chain [54].<sup>14</sup> Additional developments include the Global Maritime Distress and Safety System (GMDSS) and INMARSAT.<sup>15</sup>

Despite all the technological developments, accidents still occur. While the maritime industry has looked to technology to resolve its problems, the problems remain. There is a tendency towards the notion that only technology is allowed to promise progress and that replacing technological products with manual operators is a step backwards [21]. However, technology can increase human risk and the susceptibility for human failure by increasing the complexity and creating a more tightly coupled system. Even though major technological advances have occurred and been implemented, the attribution of human error has remained relatively constant over the past 20 years. There seems to exist the phenomenon of 'risk homeostasis' [22]:

...that advances in technology lead to a reduction in perceived risk, hence to behavior that is closer to the limits of acceptable performance--thereby effectively reducing the margin for safety.

When radar was introduced to the maritime industry, it was thought that collisions would be eliminated. Now there are radar assisted collisions. In one study, it was discovered that when initial detection was made by radar, the vessels made as many course changes in the direction of the target as away from it [38]. We are now beginning to see GPS assisted accidents.<sup>16</sup> Because of the lack of standards for GPS equipment, in conjunction with a lack of proper training, it is likely that the GPS assisted collisions will increase.<sup>17</sup>

There is an apparent coupling between erroneous actions and system complexity. Many accidents are induced by failures of technological systems, which seem to arise from the complexity of the systems themselves [42]. The introduction of technology to reduce human failures leads to more complexity; hence, more failures. Hollnagel [22] refers to this as the *Law of Unintended Consequences* (Figure 4-5).

---

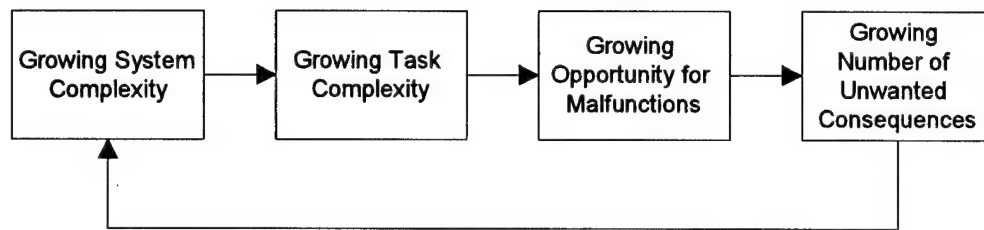
<sup>13</sup> The potential of ECDIS is immense. It could be linked via satellite to enable automatic updating of chart information. Additionally, there is potential to integrate ECDIS into all facets of marine navigation and piloting systems--ARPA, GPS, fathometer, auto-pilot, etc.

<sup>14</sup> IMO has generated a set of Facilitation messages that can be used to send information such as crew lists and cargo declarations to port authorities, customs, immigrations, etc. The UN is developing the Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT). New York and New Jersey have established the Automated Cargo Expediting System (ACES) to replace booking forms, delivery orders, arrival notices, demurrage guarantees, and bill of lading details etc. [54].

<sup>15</sup> INMARSAT, established by the International Maritime Satellite Organization, allows the transmission of voiceband data, facsimile, telex, and high speed transmissions from sea to shore via satellite.

<sup>16</sup> The recent grounding of the *Royal Majesty* is an example of a GPS assisted accident.

<sup>17</sup> Conversation with Singh.



**Figure 4 - 5: Law of Unintended Consequences**

Shipboard technology has typically been used to reduce the manning and insulate the operators that remain. As the trend toward manning reduction continues, it is not clear that there is a trend to increase the personnel standards of the remaining mariners. "Perhaps it is time to look at the person rather than the machine" [54].

## 4.9 Summary

Human failures encompass more than individual errors. The tendency to classify all human failures as individual errors has led to the notion that these failures are a part of human nature; as long as humans operate ships, there will be individual errors.

While the importance of human failure has been known, little has been done to effectively address it. Given a consistently high human failure rate, the natural corollary has been which human. The resulting quest for a human to blame has become a justification for existence for many investigation systems [52]. Post accident investigations, which find human failures, tend to limit human failure to the front-line operator rather than to search for the underlying reasons that the operator erred. Investigations have focused on placing blame rather than on determining the underlying factors contributing the accident [6].

Studies spanning 20 years have identified consistent factors contributing to human failure and individual error. While nearly all of these factors have been addressed in some form throughout the industry, most of these factors persist as pathogens.

Figure 4-6 shows the world's vessel losses by tonnage for the years 1988 to 1992 [25]. Given the high attribution of these accidents to human failure and individual error, millions of tons, and hundreds of lives, can be saved if a concerted effort is undertaken to understand the human element. Once understood, high-leverage factors can be identified and limited resources can be allocated to minimize human failures, individual errors, and their effect.

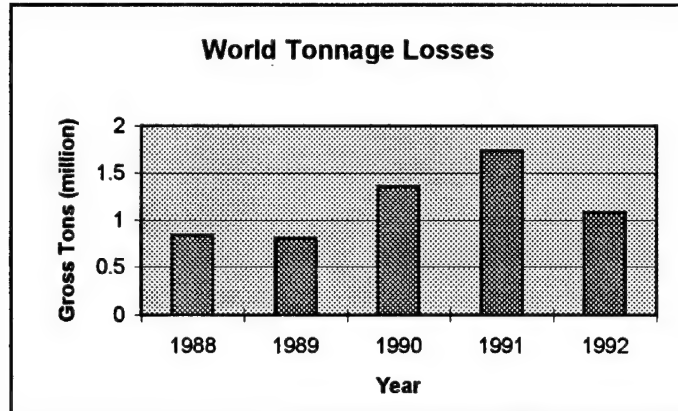


Figure 4 - 6: World Tonnage Losses 1988 - 1992

Studies of the role of human failures in engineered structures have shown that they are inevitable [5]. While there may exist the phenomenon of risk homeostasis, the appropriate attention to management and technology in the design, construction, and operations phases of the system can minimize the frequency of undesirable consequences.

Unfortunately, there are several technical problems in trying to assess human reliability in a risk setting. Human risk assessment is a relatively new discipline [12]. Rather than properly address human failure, the industry has focused on technological and structural fixes of the ship and punitive models aimed at the operators to address accident prevention.

Difficulties in addressing human failures are directly attributable to the lack of sufficient data in accident reports. In spite of the near constant 80 percent human failure rate ascribed by accident reports, there has been little or no effort expended on classifying the failures.

By conducting a PRA and integrating a Human Reliability Analysis (HRA), insight can be gained into the problems presented to and by people aboard ships. The HRA allows the analyst to look at human failure and individual error as events whose causes can be investigated rather than invoking a stop rules at the events themselves and placing blame on the person or persons performing the events. Quantitatively, human failure factors are typically the largest source of uncertainty in a PRA, but they do identify specific areas for potential risk reduction and offer insight into possible risk reduction schemes.

## Chapter 5 Human Reliability Analysis

### 5.1 Methodology

The significance of human failures and individual errors in the scope of system failures has been illustrated in the previous chapter. The field of human reliability analysis has been generated to more accurately assess the quantitative value of an individual's performance and the associated factors impacting that performance.

It is necessary to employ a human reliability analysis (HRA) technique that integrates into the PRA. The most popular methods of analyzing individual reliability involve the decomposition principle. The basic technique is to break the system down into its constituent elements, or events, and to assign reliability estimates to those elements and then to compute the aggregated result [22]. The Technique for Human Error Rate Prediction (THERP) provides that HRA scheme

### 5.2 THERP

The THERP approach is a method to predict individual error rates. It is the most widely used approach in HRA [17]. The THERP method allows the analyst to evaluate the degradation of the human-machine system likely to be caused by: either individual errors alone or with equipment functioning; operation procedures and practices; other system and human characteristics that can influence system behavior [58]. It combines a modeling method with a series of data tables containing basic human error probabilities (HEP) rates that are modified by a series of performance shaping factors (PSFs). The original data used to support the model was obtained from a series of observations and trials conducted at the Sandia National Laboratories.<sup>18</sup>

The approach is similar to a traditional system reliability analysis modified to account for possible individual error. Rather than generate equipment system states, it produces possible human task activities and the corresponding error possibilities [33].

The required steps for a THERP analysis are as follows [58]:

1. Define system failures of interest.
2. List and analyze the related human operations (task analysis).
3. Estimate the relevant error probabilities.

---

<sup>18</sup> The tasks that initiated THERP involved bomb assembly in a U.S. military facility [D4].



4. Estimate the effects of individual errors on the system failure events.
5. Recommend changes to the system and recalculate the system failure probabilities.

The following paragraphs outline the methodology utilized to incorporate the above steps into the PRA for grounding.

### **5.2.1 Define System Failures of Interest**

Recall the goal of the PRA is to identify the risks of accidental oil outflow from oil tankers. Reference [1] identified four principal failure modes:

1. Grounding.
2. Collision.
3. Structural.
4. Fire/Explosion.

Of these failure modes, groundings were investigated because of their significance as a source of accidental oil outflow. An analysis of the tanker as a system resulted in the grounding fault tree. From the fault tree, significant human interactions and task characteristics are identified for further investigation. Of the 32 elements that comprise the group of minimal cut sets in the grounding fault tree, 19 are directly related to human failure. The failures of interest that require further investigation will come from the set of 19 related human failures.

### **5.2.2 List and Analyze Related Human Actions**

From the fault tree, processes need to be identified that incorporate the failures of interest--task analysis. Task analysis is an analytical process for determining the specific behaviors required of an individual within a system [58]. A task has certain associated requirements that are performed in a specific environment and require a certain degree of intellectual and psychomotor skills. In THERP, a task is a minimal set of human actions that accomplishes a specific goal--a series of actions or steps. A deviation from an intended task step is an error.

There must be a systematic description of the appropriate actions that the individual is expected or required to carry out and the possible deviations from the requirements. The basic steps of a task analysis are as follows:

1. Evaluate the capabilities and limitations of the personnel performing the tasks.
2. Evaluate the tasks.
3. Determine possible deviations from the anticipated tasks.
4. Determine possible recovery actions.

The most difficult aspect of the task analysis is identifying the possible unplanned modes of operator response. Once the possible human errors have been determined for each task and subtask, there must be a consideration for human recovery actions (recovery from an abnormal event or failure). It must be remembered that even the best analyst cannot identify all possible modes of human response [58]. Therefore, it is important to identify the most important tasks and most of the ways performance failures can occur for the respective tasks.

The basic tool used to model tasks and task sequences is the event tree. THERP analyses incorporates event trees. Decision processes are modeled as binary events; either the task is a success or a failure. In contrast to fault trees, which are deduced from an end state, event trees work forward in time. Event trees indicate the success paths and the plausible failure paths. That is, according to time sequence or procedural order, the event tree represents the sequence of intended actions and possible alternative actions in response to an initiating event. The events must be sufficiently decomposed into small enough elements for which there is sufficient reference data to estimate probabilities.

Inherent with a task analysis is a determination of whether the demands of the system exceed the capabilities of the human components. Hence, fundamental to a task analysis is the determination of the skill, experience, training, and motivation of the personnel who will operate the system [58].

Probability shaping factors (PSFs) are those factors that affect the ability of personnel to carry out tasks [17]. Incorporated in the task analysis, is a determination of those factors that adversely affect human performance. Once tasks have been decomposed, it should be easier to identify the PSFs that influence the performance of the task. The context of PSFs and their applicability to this analysis are discussed in paragraph 5.3.

### **5.2.3 Estimate Relevant Error Probabilities**

For those human performance elements analyzed, it is necessary to determine the probability of the individual(s) to error and the influence that the hardware, procedures, environment, organizations, and the respective interfaces have on the individual(s). The error probabilities are required for the branches in the event tree. THERP contains a data source for estimating individual error probabilities in reference [58]. Once the individual error probabilities are incorporated in the event tree, the overall reliability of the task can be calculated.

### 5.2.4 Estimate the Effects of Error on System Failure Events

The results of the event trees are incorporated into the system fault tree to ascertain the probability of the undesired events in the fault tree and ultimately, the probability of grounding.

Once the appropriate probabilities are incorporated into the fault tree, a sensitivity analysis is performed to determine which event offers the largest potential for reducing the probability of grounding. Conversely, the sensitivity analysis shows those events that can significantly increase the probability of grounding.

### 5.2.5 Recommend Changes to System Design

The high-leverage factors identified in the sensitivity analysis are analyzed to determine methods that may minimize the individual event probability of failure, or at least prevent increasing the probability of failure.

Figure 5-1 graphically shows the process for incorporating the elements described above.

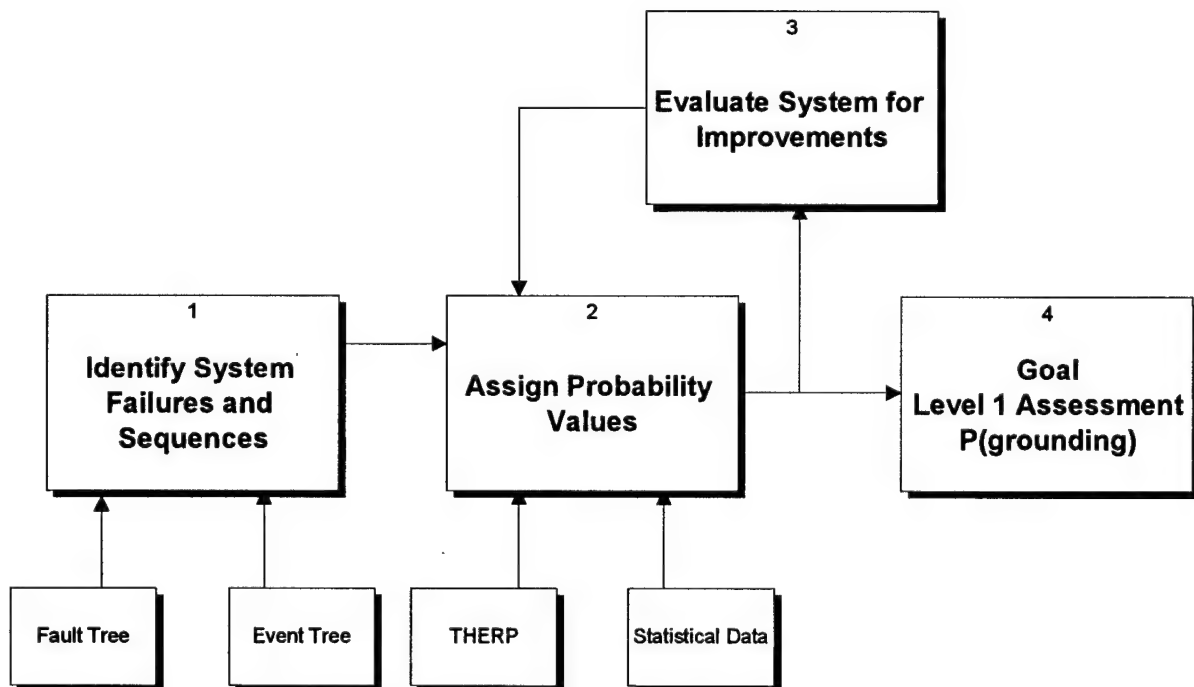


Figure 5 - 1: Probability Determination Process

### 5.3 PSFs

As stated previously, PSFs are determined inherently in the task analysis, and they identify factors that affect the ability of personnel to carry out tasks. Data relating PSFs to HEPs is scarce. Because of the nature of the probability determination for individual events in this thesis, e.g., determining marine task probabilities from analogous nuclear power tasks, explicit quantitative impacts of PSFs on individual tasks will not be determined. Instead, a sensitivity analysis will be done to determine those events that require more investigation. Recommendations will be based upon the results of the sensitivity analysis. While the use of quantitative PSF impact is not utilized, a discussion of PSFs is germane.

The manner in which the individual perceives, thinks about, and responds to the inputs he receives, depends on the PSFs. The PSFs become important when looking for means of improving performance [17]. It is essential to the HRA that the proper PSFs be identified to determine the effect external influences have upon the individual and to minimize the adverse effects. Table 5-1 shows the PSFs from NUREG1278 [58].

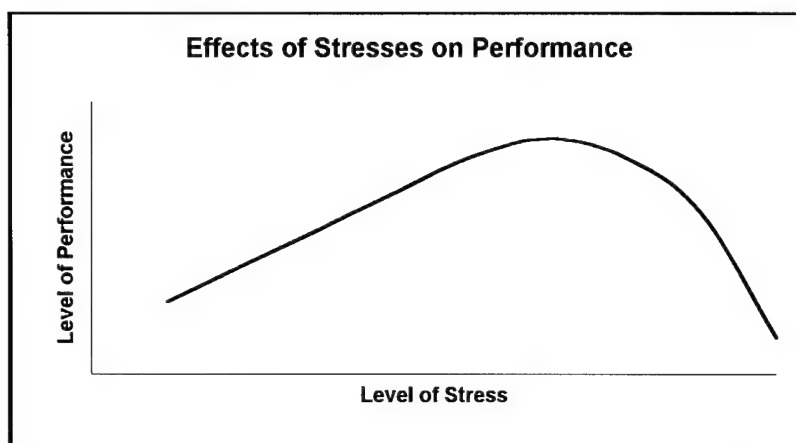
The PSFs determine whether individual performance will be highly reliable, highly unreliable, or at some level in between [58]. Recall the PSFs identified in Table 3-1. There is very little data to support the quantification of many of the cited PSFs [58]. Additionally, many of the PSFs result in various degrees of stress upon the individuals involved with the task at hand. The question remains, what degree of stress does each of the stress producing PSFs induce?

A stressor is defined as any external or internal force that causes bodily or mental tension [58]. As such, stress can be classified by its two sources: physiological and psychological. Stress is not necessarily undesirable. It has been shown that there are optimum levels of stress to maximize the performance of individuals.

The relationship between psychological stress and performance is shown in Figure 6-2 [2]. A certain level of stress will maximize the level of individual performance. As stress increases, the performance of most people will deteriorate rapidly. A particular problem under high levels of stress is that of response perseveration--"the tendency to make some response (or a very limited number of responses) that is incorrect repeatedly" [58]. Perseverate behavior can result from either the lack of skills to adequately process the information at hand, or from an inability to recall and use the appropriate skills. In either case, the training and experience level of the individual impact that individual's performance level during periods of high stress.

**Table 5 - 1: Performance Shaping Factors**

Procedures			Stressors		Internal
Situation	Job and Task Instructions	Task and Equipment Characteristics	Psychological Stressors	Physiological Stressors	Organismic
Architectural Features Quality of Environment Work Hours/Breaks Availability/Adequacy of Equipment Manning Parameters Organizational Structure Actions by Supervisors Rewards, Recognition, Benefits	Procedures Required Written or Oral Communications Cautions and Warnings Work Methods Policies	Perceptual Requirements Motor Requirements Control-Display Relationship Anticipatory Requirements Interpretation Decision-Making Complexity Narrowness of Task Frequency and Repetitiveness Task Criticality Long and Short-Term Memory Calculation Requirements Feedback	Suddenness of onset Duration of Stress Task Speed Task Load High Jeopardy Risk Threats Monotony Long, uneventful vigilance periods Conflicts of Motives Reinforcement absent or negative Sensory Deprivations Distractions Inconsistent Cueing	Duration of Stress Fatigue Pain or discomfort Hunger or Thirst Temperature Extremes G-force Extremes Atmospheric Pressure Extremes Oxygen Insufficiency Vibration Movement Constriction Lack of Physical Exercise	Training/Experience Proficiency Personality/Intelligence Variables Motivation/Attitude Knowledge of Required Performance Standards Physical Condition Outside influences Group Identification



**Figure 5 - 2: Effects of Stresses on Performance**

At the lower extreme of the stress level, the performance levels of most individuals will also decrease. Since low levels of stress do not offer enough arousal to keep a person sufficiently alert to do a good job [58]. Swain [58] calls this loss of alertness the vigilance effect--ineffective monitoring that develops when the operator is not experiencing enough signals to maintain a sufficient level of stress.<sup>19</sup>

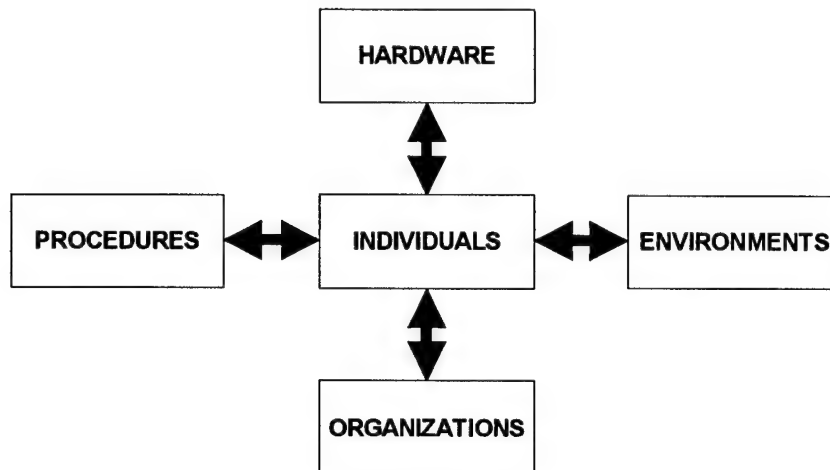
The primary physiological stressors applicable to the mariner are from fatigue, motion sickness, and the duration of either the psychological or physiological stress that the mariner must endure. When an individual must perform under physically uncomfortable conditions, errors of omission can be expected to increase [58].

Despite the ambiguity of the PSFs and the variability of human performance, it is still important to identify contributing PSFs. Therefore, for the human failure causal factors identified in Table 5-1, PSFs will be identified, within the human failure taxonomy, that can affect the individual's performance.

### **5.3.1 PSF Considerations**

Recall that human reliability is affected by all the synergistic and antagonistic effects of hardware, procedures, environment, organizations and the interfaces of these with the individual (Figure 5-3) [3].

<sup>19</sup> In World War II, the British realized that the maximum time that a ship's lookout could be kept on duty effectively was about thirty minutes. After thirty minutes, the probability of the lookout detecting an enemy submarine's periscope was unacceptably low even though the lookout's life and those of his shipmates were at stake [58].



**Figure 5 - 3: Human Failure Factors**

All of the above listed items come with inherent factors that affect the ability of personnel to carry out tasks.

### **5.3.1.1 Hardware**

The bridge design of a ship can affect the performance of individuals either favorably or adversely. The bridge size of most tankers is significant. Therefore, the location of vital navigational equipment (radar repeaters, communications, gyro repeaters, rudder angle indicators, charts) should all be readily accessible to the conning officer. Since it is normal for people to avoid unnecessary effort, they may try to read displays from a distance and make errors in their readings [58]. These issues are especially prevalent in older tankers that were not designed with contemporary manning levels taken into consideration. Many older tankers were designed with the chart room separate from the bridge.<sup>20</sup>

The perceptual requirements of a task are determined by the task and the equipment features that convey information to the individuals [58]. Therefore, crucial information must be reliably conveyed with the essential information to the conning officer.<sup>21</sup> In general, the hardware must be designed such that it interfaces properly with the individuals utilizing it.

<sup>20</sup> On a recent tanker visit, the chart room was behind the bridge in a separate room. This required the conning officer to leave the advantageous view of the bridge to plot fixes. This behavior was restricted to open ocean steaming. For restricted water piloting, the crew utilized a smaller table on the bridge. The problem with this table is that there was no light fixture. As a result, flashlights with white lights were turned on and off to plot fixes and compare the ship's position with the track. This behavior was distracting and reduced the night vision of all personnel on the bridge.

<sup>21</sup> ARPA radars beep in certain modes with certain data entries. Again, on the same tanker visit, it was difficult to distinguish the ARPA radar beep from the steering alarm which occurs when the rudder angle indicator fails to respond to the ordered angle promptly.

The primary PSFs to be considered are:

1. Architectural Features (bridge design).
2. Perceptual Requirements (placed on personnel by the equipment).

#### **5.3.1.2 Environment**

The marine environment can be harsh. High sea state conditions can severely affect the performance of individuals through physiological stressors, particularly if the individual suffers from motion sickness. Even if motion sickness is not a problem, enduring days of high sea state takes its toll in the form of fatigue and stress as sleep becomes difficult. Motion sickness is typically constrained to the open ocean. It is more important to identify those environmental factors affecting performance in restricted waterways. The environmental factors contributing to the performance of piloting a vessel include the shipping channel width, traffic density, prevailing currents and winds, visibility, and the availability of navigational aids.

The primary affect of the above factors on the individuals piloting a ship is to change the amount of stress. The mariner can spend days, or weeks in an open ocean transit where the risk of a grounding or collision are almost nonexistent and the margin for error is relatively large. But then there is a sudden transition to a restricted waterway where there can be a significant traffic density to avoid while contending with current and wind forces on the ship and maintaining a safe track through the use of navigational aids and radar fixes. In addition to the stress associated with operating in a restricted waterway, there is stress induced as a function of the rapid transition from open ocean to restricted waters. The particular stressors placed upon the mariner due to the environment are:

1. Suddenness of onset.
2. Duration of stress.
3. Long uneventful vigilance periods.
4. Distractions.
5. Inconsistent cueing.

#### **5.3.1.3 Organization**

The organizational structure (authority, responsibility, and communication channels) of the ship and the corporate management for the ship impact the performance of the ship's operators. Goals set by an organization can lead a rational individual to conduct operations



which corporate management would disapprove of if they were aware of the reliability implications [3]. Pressures to reduce costs and maintain schedules can either provide the motivation for operators to take greater risks, or may not provide the adequate resources for operators to function with a sufficient safety margin.

Administrative control, with regard to procedural compliance, is necessary to ensure that abnormal conditions are restored properly. The perceived criticality of the task at hand determines how much attention an individual will devote to the task [58]. A conning officer's perception of importance will be directly influenced by the Captain and the prevailing attitude's of the experienced personnel on board.

Rewards, recognition and benefits serve to provide the incentive for an individual to perform in accordance with the organization's goals. These serve to affect an individual's decision criteria and how these criteria are used [3].

The bridge team structure affects the interaction of the individuals that make up the team. By encouraging interaction, the principle of redundancy is employed. Additionally, once an error occurs, recovery action is more likely.

The above effects on an individual's performance can be summed up in the single PSF:

1. The Organizational Structure.

#### **5.3.1.4 Procedures**

The design and adherence to properly written procedures can lessen the interpretation requirements placed upon an individual. The more interpretation that is required, the longer the response time, hence the greater probability of error [58]. One of the most important work methods is the correct use of properly written procedures and checklists. The shipboard environment typically suffers from the lack of procedures, rather than the lack of adequate procedures.

The nautical rules of the road are a common factor to all mariners. Adherence to the rules is more likely a function of the organizational structure. Therefore, the prevailing PSF is:

1. Existence and quality of procedures and checklists.

#### **5.3.1.5 Individuals**

The scheduling of work hours and work breaks are unique in a sea duty environment. Watchstanding must be coupled with maintenance and repair activities. When loading and unloading cargo are coupled with scheduling pressures, time stress can occur. Individual performances are degraded when the body's circadian rhythms are disrupted.<sup>22</sup> In addition to the stress that can be induced from long work hours, fatigue becomes a critical matter. The required work hours are directly affected by the ship's manning. Reduced manning initiatives have required fewer people to do more jobs. Studies have shown that as fatigue increases, the detection of visual signals deteriorates and individuals exhibit more errors [58].

The piloting of a ship requires the conning officer to be alert to many signals. Individuals are only capable of paying attention to one thing at any instant in time [58]. Experience allows the individual to switch attention among several stimuli, however, the individual is attending to just one stimulus at a time. In a restricted maneuvering channel with high traffic density, there may be too many auditory and visual signals competing for the conning officer's attention that an information overload can occur. As a result, some signals will either not be perceived, or they will be ignored because of the priority of other signals. Feedback refers to the knowledge of results that a person receives about the status or adequacy of his or her outputs [58]. The information processing by individuals requires a closed loop to reliably perform complicated activities. Specifically, feedback provides an individual with objective information on what is supposed to be done, and whether it is done correctly, with detailed information on when and how the individual failed to do the task correctly [58]. When feedback delays occur, it becomes difficult to see the association between feedback and intervening events [51]. Slow feedback is inherent to the piloting of large vessels. The maneuvering characteristics of large vessels are such that they respond slowly to the control inputs. Because of the feedback delay, it takes a great deal of experience and a minimum level of proficiency to be able to properly maneuver a large vessel.

The primary internal PSFs operating on the individuals reliability are:

1. Fatigue.
2. Experience and training.
3. Proficiency.

---

<sup>22</sup> Studies done to determine the effects of the standard three-watch rotation (four hours on watch, eight hours off) have concluded that crew member's circadian rhythms are disrupted resulting in sleep deprivation. The results have shown a degraded performance in monitoring and judgment and increased stress [37].

### **5.3.2 PSF Synopsis**

The primary PSFs that act upon and within an individual mariner to effect the reliability of that mariner, are as follows:

1. Bridge Design.
2. Equipment Ergonomics.
3. Stress Placed on the Individual due to the environment.
4. The organizational structure.
5. The existence of procedures and checklists.
6. Fatigue.
7. Experience and Training.
8. Proficiency.

Just as important to identifying the PSFs, is identifying the means for either reducing or eliminating the adverse impact that the PSFs can have upon an individual.

In order to better ascertain the relevant PSFs, the analyst should actually perform the tasks according to the prescribed procedures to evaluate the human processes involved in performing each of the events within the task. It is this hands-on experience that lends the analyst insight into the appropriate PSFs and the potential impact on each event within the task.

## **5.4 THERP Critics**

Critics of THERP, question the underlying assumptions in the approach. It assumes that a task can be broken into discrete events, and that each event in isolation is not significantly different from the task as a whole. While this decomposition principal has its weaknesses, it is a systematic approach to an industry-wide problem, and it has shown success in identifying areas for improving human reliability. Additionally, there is a question of validity when using THERP for evaluating either high level decisions, or diagnostic tasks. While there is truth in the criticism, THERP does provide a starting point for the maritime industry where data relating cognitive psychology to the process of marine transportation is non-existent. Therefore, the resulting absolute risk likely incurs a large margin of error, however, the relative risk serves to offer insights into the ways that the absolute risk can be minimized using sensitivity analyses as a way to identify vulnerabilities, which may be subsequently removed.

## 5.5 Summary

Familiarization is fundamental to the THERP method. Familiarization includes information gathering, ship visits and the review of procedures. Hence, site data collection is essential to the risk assessment [17].

Many tasks inherent with piloting a ship are not well defined. Even in routine tasks, there are myriad possible deviations from the anticipated routine. For tanker groundings, the tasks that make up the cut sets of the fault tree must be analyzed such that they can be broken down into fundamental steps for which probabilistic data can be applied. Once the steps are quantified with HEPs, the sensitivity analysis allows managers, regulators, and operators to focus on the high-leverage factors to minimize the overall risk of grounding.

## Chapter 6 Probability Determination

### 6.1 The Grounding Fault Tree

Recall the grounding fault tree (Figure 6-1) [1]. From the fault tree, causality can be broken into two broad categories:

1. *Planning and piloting*: the vessel is able to follow a safe track, however, it proceeds down an unsafe track due to a planning or piloting failure.
2. *Equipment, assistance and environment*: the vessel is unable to follow a safe track because of mechanical failure, assistance failure and adverse environmental conditions.

The above breakdown is consistent with a study done by Det Norske Veritas (DNV) [11]. DNV has defined the two categories as follows:

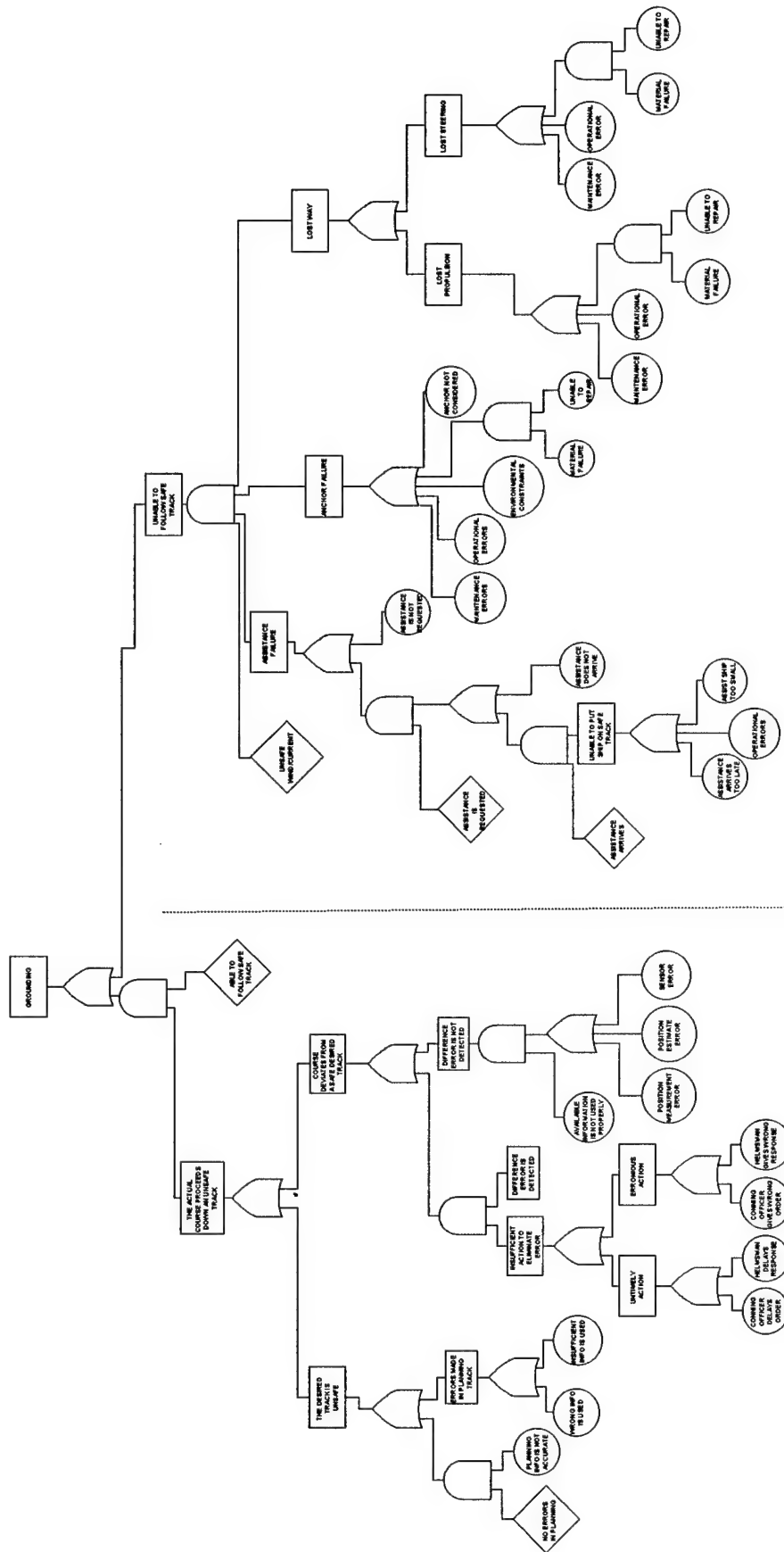
1. *Powered grounding*: An event type that occurs when a tanker collides with the shoreline whilst underway due to navigational error and lack of crew vigilance.
2. *Drift grounding*: An event type that occurs when a tanker loses its ability navigate, through loss of steering or propulsion, and is blown onto the shoreline before it is either taken in tow or is repaired.

The causality derived by the fault tree is consistent with the grounding definitions developed by DNV. For consistency and clarity the DNV terms are used to describe the two broad causal categories. The OR gate immediately preceding the grounding event in the fault tree has an input from the powered grounding portion of the fault tree and an input from the drift grounding portion of the fault tree. Therefore, the Boolean expression for the probability of grounding can be restated as follows:

$$P(\text{grounding}) = P(\text{powered grounding}) + P(\text{drift grounding})^{23} \quad (6-1)$$

---

<sup>23</sup> As a Boolean expression, it is read as: The probability of grounding is equal to the probability of powered grounding OR the probability of drift grounding. As shown in Appendix A, a union operation expressed as a Boolean OR operation is implicitly equal to the probability expression:  $P(C) = P(A) + P(B) - P(A * B)$ .



## DRIFT GROUNDING

## POWERED GROUNDING

Figure 6 - 1: Grounding Fault Tree

From equation (6-1), P(powered grounding) and P(drift grounding) have the following identities that are implicit from Figure 6-1:

$$\begin{aligned} \text{P(powered grounding)} &= \text{P(the actual course proceeds down an unsafe track)} \\ &\quad * \text{P(the ship is able to follow a safe track)} \end{aligned} \quad (6-2)$$

$$\begin{aligned} \text{P(drift grounding)} &= \text{P(the ship is unable to follow a safe track)} \\ (6-3) \end{aligned}$$

Notice the P(the ship is unable to follow a safe track) is the negation of P(the ship is able to follow a safe track). Through Boolean identities, P(grounding) is expressed as follows:

$$\begin{aligned} \text{P(grounding)} &= \text{P(powered grounding)} + \text{P(drift grounding)} \\ &= \text{P(the actual course proceeds down an unsafe track)} \\ &\quad + \text{P(the ship is unable to follow a safe track)} \end{aligned} \quad (6-4)$$

### 6.1.1 The Emphasis on Powered Grounding

Based on the analysis of 100 accidents at sea,<sup>24</sup> Groeneweg [20] concluded that 96 of the accidents were preceded by human failures. There were 345 necessary human failures identified.<sup>25</sup> Out of all the identifiable and necessary human errors, 76 percent of these errors occurred on the bridge.

Since the bridge is the controlling station for the ship, it is not surprising that the majority of contributing events preceding an accident are attributable to the actions taken on the bridge. "Therefore, programs to improve safety should look carefully at what happens on the bridge" [20].

The significance of the bridge and the actions taken there, is reflected in the number of marine accident causal factors attributed to this controlling station of the vessel. This is substantiated by the grounding fault tree. From Figure 6-1 and equation (6-4), the Boolean expression for the grounding event is taken to the next level to show the importance of the bridge.

$$\begin{aligned} \text{P(powered grounding)} &= \text{P(the desired track is unsafe)} \\ &\quad + \text{P(the course deviates from a safe desired track)} \end{aligned} \quad (6-5)$$

$$\begin{aligned} \text{P(drift grounding)} &= \text{P(an unsafe wind/current)} \\ &\quad * \text{P(an assistance failure)} \\ &\quad * \text{P(anchor failure)} \\ &\quad * \text{P(ship has lost way)} \end{aligned} \quad (6-6)$$

<sup>24</sup> The 100 accidents at sea are all cases heard by the Dutch shipping Council between 1982 and 1985. For an accident to be heard by the Council it had to either involve a fatality or be of major interest to the community or marine industry. There were 2250 accident causes identified, out of which 345 were forms of human error [20].

<sup>25</sup> Necessary human failures implies that these failures were necessary for the accident to occur.

The Boolean expression for the probability of grounding can now be expressed as:

$$\begin{aligned} P(\text{grounding}) = & (P(\text{the desired track is unsafe}) + P(\text{the course deviates from a safe desired track})) \\ & + (P(\text{an unsafe wind/current}) * P(\text{an assistance failure}) * P(\text{an anchor failure}) \\ & * P(\text{the ship has lost way})) \end{aligned} \quad (6-7)$$

The above equation is stated as a Boolean expression.<sup>26</sup> By invoking the rare event approximation and assuming independence (see Appendix A for the details of Boolean algebra, probability theory, and the rare event approximation), the Boolean expression of OR's and AND's translates directly to a mathematical expression of addition and multiplication. Therefore,  $P(\text{the desired track is unsafe})$  is summed with  $P(\text{the course deviates from a safe desired track})$ , and this quantity is then summed with the product of  $P(\text{an unsafe wind/current})$ ,  $P(\text{an assistance failure})$ ,  $P(\text{an anchor failure})$ , and  $P(\text{the ship has lost way})$ .

Since the probabilities are all less than or equal to 1 (including  $P(\text{grounding})$ ), the product term ( $P(\text{drift grounding})$ ) will be less than the maximum probability within the product. Given the nature of the probabilities in the product term, one can see the importance of the sum term ( $P(\text{powered grounding})$ ).

The bridge will be the center of focus for further analysis. Event trees will be developed to determine the failure probabilities of powered grounding. Due to time constraints, the probabilities of drift grounding will be based upon historical data.

## 6.2 Powered Grounding

The powered grounding fault tree is shown in Figure 6-2. It can be seen that the fundamental failures resulting in a powered grounding lie in the processes of planning and piloting. Those elements of the fault tree extending from "The Desired Track is Unsafe" constitute faults in the planning process. Likewise, those elements extending from "Course Deviates from a Safe Desired Track" are characteristic faults of the piloting process.

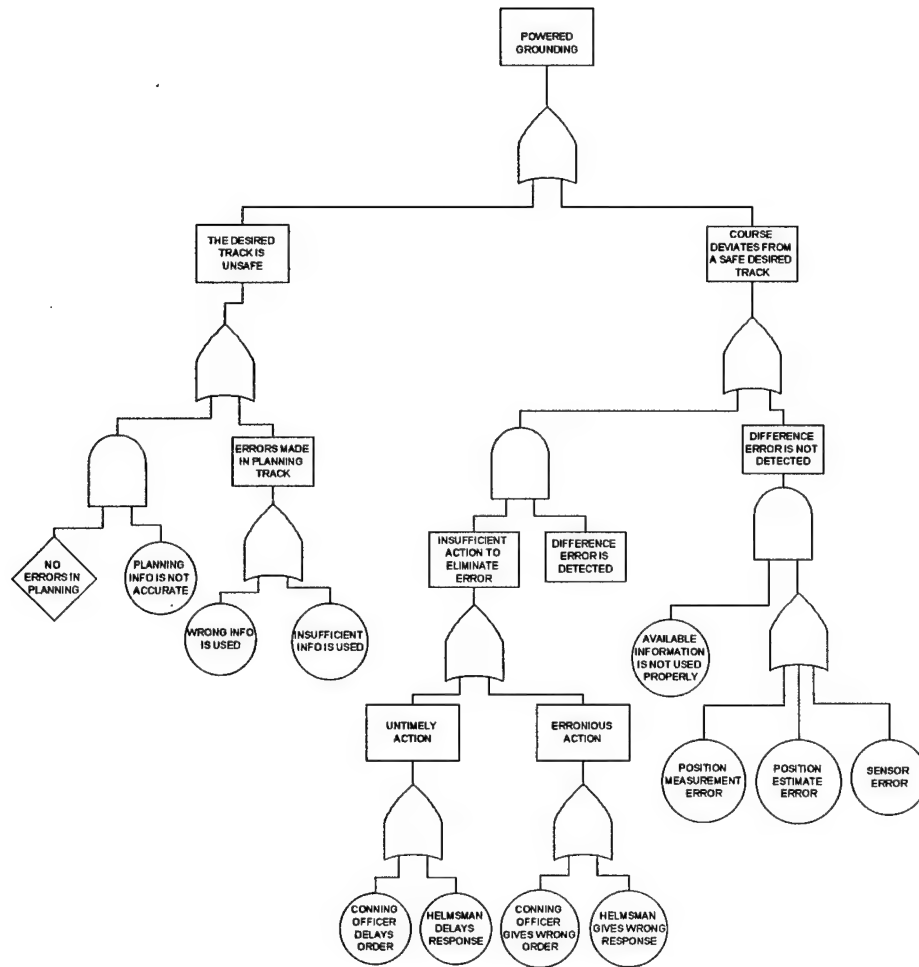
Voyage planning and piloting are essential skills required of any mariner. Event trees can be used to further analyze and quantify portions of the fault tree. By developing event trees for each of these processes, the fundamental events of each of the processes are sequenced. The sequence of the events involved with the processes incorporate the basic faults identified in the fault tree. From the event trees, the probabilities of either success, or failure of each of the processes, or elements of the processes can then be calculated.

When events are human actions, probabilities will be determined from reference [58]. Excerpts of the tables from reference [58] used in this analysis are included as Appendix C, however, for further insight into each of the elements of the tables in Appendix C, it is recommended that one refer directly to reference [58].

---

<sup>26</sup> As a Boolean expression, "+" are read as OR, and "\*" are read as AND.





**Figure 6 - 2: Powered Grounding Fault Tree**

### 6.2.1 Passage Planning

The process of voyage planning requires the scheduling of escorts, tugs, and pilots for both departure and arrival ports. However, the essential element of a voyage plan is the passage plan.

The mariner has several sources of information available to ensure a safe and efficient passage. The failure to have on board the latest charts and other publications, and to keep them corrected imposes undue hazards to the crew and vessel, in addition to the adverse legal position should a mishap occur.

The passage plan requires the mariner to plot the vessel's intended track on the appropriate charts. The charts must be checked to ensure that they reflect the most recently known navigational information (e.g., Notice to Mariners, Local Notice to Mariners, etc.). It is im-

portant to determine if low-water conditions impact the ship. Additionally, currents can impart significant forces upon the ship. Therefore, currents and tides must be checked.<sup>27</sup>

Figure 6-3 shows a typical passage planning event tree. Recall that for each event, the success limb is the upper limb, and the failure limb is the lower.

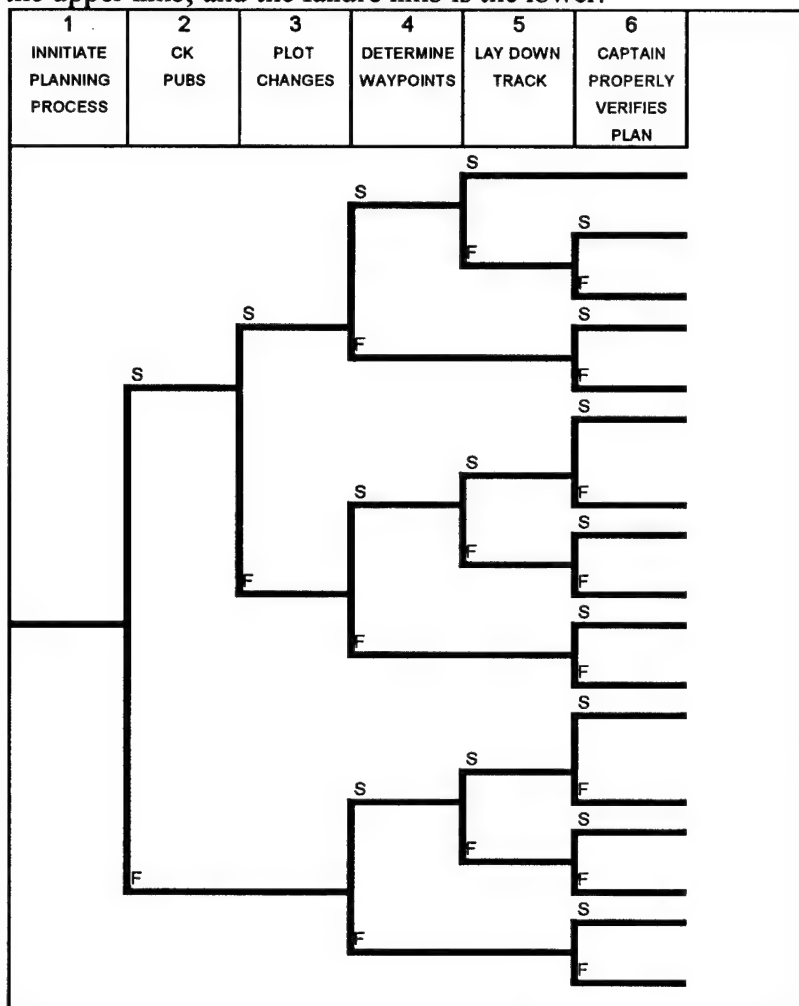


Figure 6 - 3: Passage Planning Event Tree

The process of verifying that charts reflect the most accurate navigational information involves checking various notices that are published to reflect changes in navigational information. Periodicals are issued to correct or update navigational publications. The primary periodicals are the *Notice to Mariners* and the *Local Notice to Mariners*. For instances where it is necessary, for the safety of navigation, to promulgate information without delay, a radio broadcast service is utilized. Messages used to indicate hazards are the *Hydropac*, *Hydrolant*, and the *Broadcast Notice to Mariners*.

Prior to departure and arrival, publications must be corrected as necessary to reflect the most recent changes. The process can be tedious and time consuming. To determine the HEP

<sup>27</sup> While it is necessary to check current and tide tables to get an idea of the expected currents, to ascribe any real accuracy to these tables would no be prudent.

to apply to this task, the table for "Estimated Probabilities of Error When Using Written Procedures Correctly"<sup>28</sup> from reference [58] is used. It is assumed that the process for checking the navigation periodicals and messages is analogous to the HEP for following procedures with no check-off provision.<sup>29</sup>

The HEP for correctly entering the changes in the appropriate charts and publications is taken from the same table. Since the mariner has developed a list of changes to make, the HEP is taken from the line item for procedures with check-off provisions.<sup>30</sup>

The task of determining waypoints for the passage involves studying the charts to determine the track to take the vessel from origin to destination. It is assumed that the HEP is analogous to that of preparing written procedures.

The task of laying down the track involves the plotting of the waypoints and highlighting any hazards to navigation. The process requires relatively precise use of dividers and simple mathematical calculations, analogous to a reactor technician's use of a micrometer. The Handbook categorizes these tasks under arithmetic computations.

The approval process presumes that the Captain takes a hands-on effort in verifying the validity of the track. A successful verification implies that the Captain has disapproved an improper plan. The analogous HEP from the handbook corresponds to the table for "Estimated Probabilities of a Checker's Failure to Detect Errors."

A summary of the chosen probabilities is given in the table below.

**Table 6 - 1: HEPs for Passage Planning**

<b>Event Number</b>	<b>Maritime Task</b>	<b>Analogous Nuclear Power Task</b>	<b>HEP</b>	<b>Uncertainty</b>
2	Check periodicals for changes	Procedures with no check-off provision	0.003	0.001 - 0.01
3	Enter changes	Procedures with check-off provision	0.001	0.0005 - 0.005
4	Determine waypoints	Writing a procedural item incorrectly	0.003	0.001 - 0.01
5	Plot track	Procedures requiring simple arithmetic	0.01	0.005 - 0.05
6	Captain approval	Hands-on type checking	0.01	0.005 - 0.5

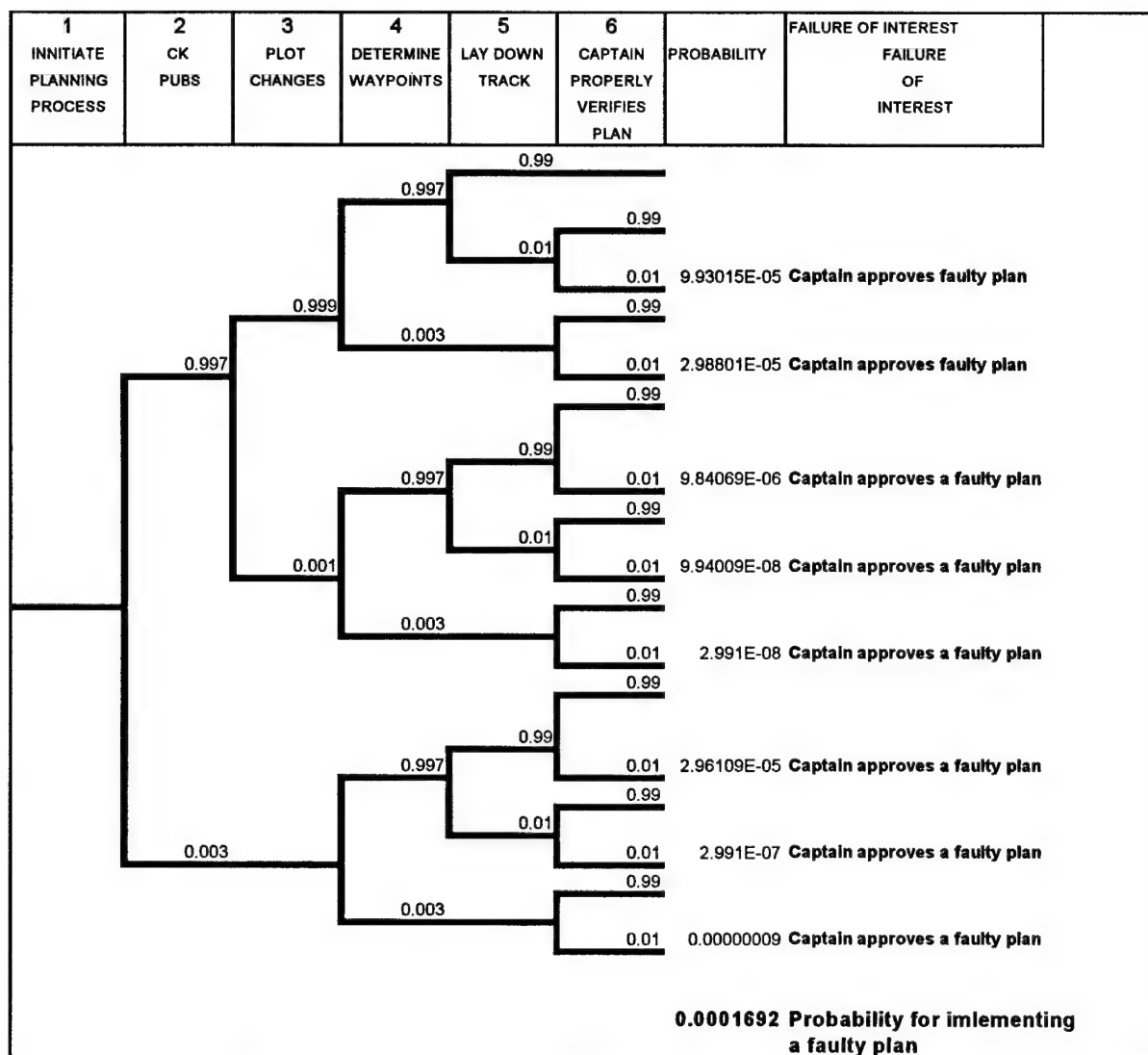
Incorporating the above HEPs into the passage planning event tree yields a resulting probability of failure of  $1.692 \times 10^{-4}$ , as shown in Figure 6-4. Failure is defined as implementing a faulty plan.

It can be assumed that the first three events are independent of each other, since it is unlikely that the successive event will induce the operator to believe that the previous event was performed incorrectly. In other words, there is no mechanism for recovery. However, the performance of event 4 does provide for recovery. It can be rationalized that in the process of plotting the track, the plotter has a general idea of the way the track will lay-out before actually plotting it, since the waypoints were determined from studying the charts. If this dependence is assumed, the event tree must model the recovery event.

<sup>28</sup> In this context, written procedures include any written materials.

<sup>29</sup> The HEP used assumes less than 10 changes have to be implemented (see Appendix C).

<sup>30</sup> It is assumed that the list is analogous to a check-list or procedure that a reactor technician might follow.



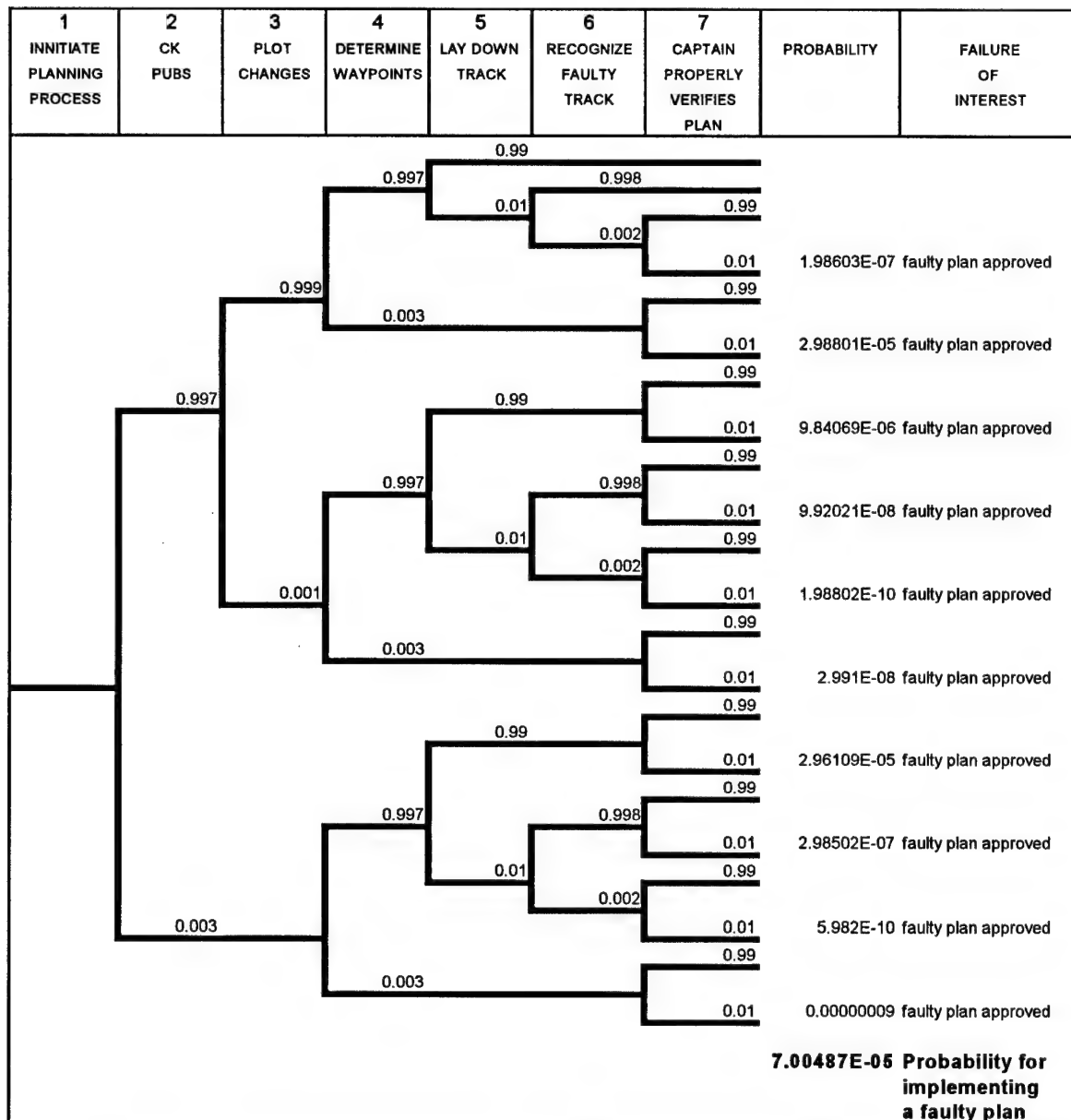
**Figure 6 - 4: Passage Planning Event Tree with Associated Probabilities**

The recovery event is the recognition of the faulty track after the track is laid-out. This presumes that the individual laying down the track is checking it for the specific purpose of meeting the constraints of a safe passage. This is analogous to the table in reference [58] for checking displays for a specific purpose. This recovery event becomes event 6 in the event tree just preceding the Captain's verification event.

**Table 6 - 2: HEP for Recognizing Faulty Track**

Event Number	Maritime Task	Analogous Nuclear Power Task	HEP	Uncertainty
6	Recognize Faulty Track	Check chart recorder with limits	0.002	0.001-0.01

Figure 6-5 incorporates the recognition event and shows that the resulting probability of implementing a faulty track has reduced by an order of magnitude--from  $1.692 \times 10^{-4}$  to  $7.0049 \times 10^{-5}$ .



**Figure 6 - 5: Passage Planning Event Tree Incorporating Plot-Waypoint Dependency**

The final probability chosen for implementing a faulty plan is  $7.0049 \times 10^{-5}$ . There are assumptions regarding the number of changes and the number of waypoints for a particular voyage. Additionally, ships on a continuous route between two ports will utilize the same track over and over again. However, the process for the prudent mariner remains the same regardless of the experience on the voyage route.

## 6.2.2 Planning Information

Inherent with evaluating the probability of the desired track being unsafe, is the determination of the probability that the information used to plan the track is inaccurate.<sup>31</sup> Only a small portion of U.S. waters have been surveyed using the most advanced techniques, and 60 percent of the soundings shown on nautical charts are based on lead-line surveys conducted over 45 years ago [35]. By conducting a search of the USCG's CASMAIN database, a rough order of magnitude estimate has been developed for the probability of piloting with faulty navigational information.

A query of the CASMAIN database was performed for the causes of vessel groundings. Interest lies in the cases where the vessel's did not have the navigational information reflecting the actual environmental conditions. It was assumed that the following causes attributed to the casualty in the database were a result on inaccurate information:

1. Channel not maintained.
2. Unmarked channel hazard.
3. Inadequate weather information available.
4. Improper navigational aid location.

The results of the query yielded 1,874 cases where vessels grounded due to false navigational information between the years 1980 and 1991. Of the 1,874 vessel accidents identified, 298 were tankers. The location for these accidents is dominated by those that occurred in rivers. This illustrates the importance for understanding river dynamics and the increased caution that must be exercised when transiting rivers.

Based upon four of the busiest ports in the U.S.--San Francisco Entrance, New Orleans, Baton Rouge, and Valdez, the number of vessel transits was obtained from the Army Corps of Engineers. For the years 1986 through 1990, the total number of transits for these ports is illustrated in Table 6-3 [64].

---

<sup>31</sup> Presently, there is a Sea Grant research project being conducted by Woods Hole Oceanographic Institution to determine the extent which accidents are caused by faulty navigational data [67]

**Table 6 - 3: Annual Vessel Trips for Selected Ports**

Port	Year	Annual Tanker Transits	Total Annual Transits
<b>Valdez</b>	1986	1790	2783
	1987	2056	2445
	1988	1941	2932
	1989	1568	2579
	1990	1678	2297
	<b>Total</b>	<b>8708</b>	<b>14398</b>
<b>New Orleans</b>	1986	1650	136948
	1987	1513	147796
	1988	1760	158102
	1989	1895	152406
	1990	734	78534
	<b>Total</b>	<b>7552</b>	<b>673786</b>
<b>Baton Rouge</b>	1986	1212	40838
	1987	1269	53612
	1988	1209	58076
	1989	1335	58194
	1990	1248	59349
	<b>Total</b>	<b>6273</b>	<b>270069</b>
<b>San Francisco Bay Entrance</b>	1986	1780	8475
	1987	2089	8938
	1988	1998	8916
	1989	2029	8730
	1990	2237	8936
	<b>Total</b>	<b>10133</b>	<b>43995</b>

The number of groundings near these ports, which were the result of incorrect navigational information, is divided by the number of transits to determine the accident quotient.

$$\text{Information Accident Quotient} = \frac{\text{Number of Accidents due to Faulty Navigational Information}}{\text{Number of Transits}} \quad (6-8)$$

The accident quotient is then assumed to approximate the probability of grounding attributable to incorrect planning information. Table 6-4 compares these quotients.<sup>32</sup>

<sup>32</sup> Because the CASMAIN database does not easily allow the distinction between Baton Rouge and New Orleans, these port trip totals are combined.

**Table 6 - 4: Incorrect Planning Information Accident Quotients**

Port	Number of Accidents	Accident Quotient	Number of Tanker Accidents	Tanker Accident Quotient
Valdez	2	$1.398 \times 10^{-4}$	0	0
San Francisco Bay Entrance	3	$6.819 \times 10^{-5}$	0	0
New Orleans/Baton Rouge	83	$8.794 \times 10^{-5}$	19	$1.374 \times 10^{-3}$
Total	87	$8.680 \times 10^{-5}$	19	$1.896 \times 10^{-5}$
Channel Weighted Mean	29.3	$9.86 \times 10^{-5}$	6.33	$4.58 \times 10^{-4}$
Standard Deviation	46.5	$3.70 \times 10^{-5}$	11.0	$7.93 \times 10^{-4}$

Based on the above quotients, it is difficult to determine any clear statistical conclusions, especially for exclusive tanker accidents. Additionally, the port characteristics are different, imposing different variables on the ships transiting the specific waterways. An approximation of  $10^{-4}$  is used as a reasonable estimate. Let the upper bound of uncertainty be determined by the number of tanker accidents in the New Orleans/Baton Rouge waterway-- $10^{-3}$ . The lower bound will then be estimated as  $10^{-5}$ . It must be noted that this failure probability disregards differences in waterway characteristics.

### 6.2.2 Piloting

The piloting event tree is depicted in Figure 6-6. The initiating event is the actual course deviating from the planned track. The simple sequence of events is as follows:

1. *The actual course deviates from the planned track.* This is the initiating event and the resulting probabilities are conditional upon this initial deviation.
2. *A difference error between the actual course and the planned track is generated.* To enable a detection of a deviation, the on board sensors must detect and offer that information to the bridge team.
3. *A fix is taken and plotted.* Once the on board sensors offer the information to the bridge team, the bridge team takes that information in the form of a fix and the fix is then plotted on a chart.
4. *The difference error is detected.* When the fix is plotted, the bridge team must evaluate the fix to detect that a difference exists between the actual position and the desired position.
5. *A correct course change is ordered.* Once the ship's deviation is recognized, a course change must be given to negate further deviation.



6. *The helm responds correctly.* The helm must respond with the proper rudder order to bring the ship's track back to the planned track.

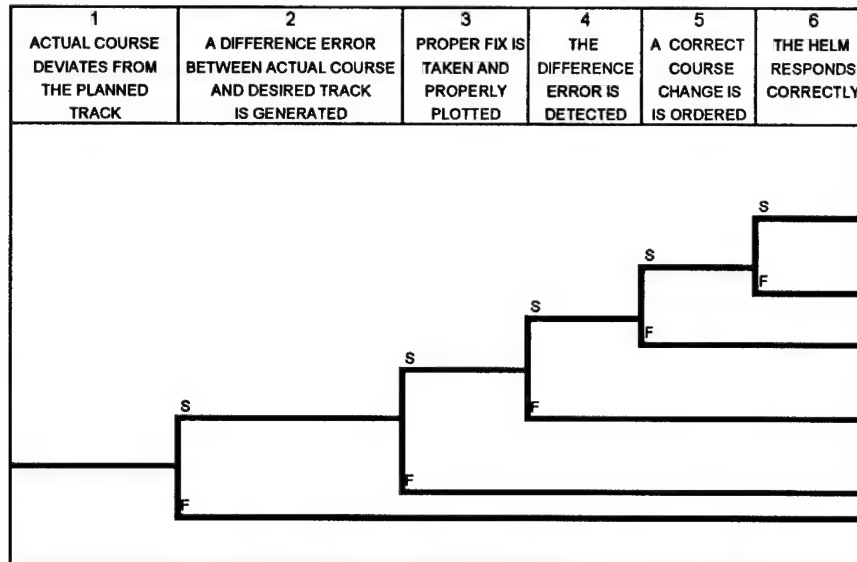


Figure 6 - 6: Piloting Event Tree

Since the merchant fleet is limited in its manning, conning officers typically rely upon radar ranges and bearings to pilot the ship through restricted waters, rather than utilizing a piloting team to shoot and plot visual bearing lines. In restricted waters, pilots embark to take the ship to the port of call. For this reason, *Dutton's Navigation & Piloting* [31] recommends that the mate performing the navigational duties in restricted waters refrain from making trips between the bridge wings, chart house and wheelhouse. Rather, it is preferable to utilize a chart table in the wheelhouse and fix the ship's position with the radar in order to keep a close check on the pilot.

The generation of a difference error between the actual course and the desired track is a function of the accuracy and reliability of the radar used to fix the ship's position and the Global Positions System (GPS). The IMO has mandated performance standards for required navigational equipment in the *International Convention for the Safety of Life at Sea* [24]. Because there are a number of systems installed on tankers, a value for the probability of generating a difference error is chosen based upon the value presented in reference [41].

The process of taking a fix typically involves the taking of at least two radar ranges. This is done by selecting appropriate navigational aids, obtaining the ranges, and then plotting those ranges. The navigator must read the ranges off of the radar and plot them correctly on the chart. The result is the estimated ship's position at the time the ranges were determined. The ranges are presented in a digital format, hence, the HEP is chosen from the table for "Probabilities of Errors of Commission in Reading Quantitative Information from Displays." The recording of the information obtained involves more than just writing down the information. Since some skill is required in using the dividers to plot the ranges at the correct scale,

the HEP for recording is taken from the table for "Probabilities of Error of Commission in Recording Readings" is taken as the higher HEP.

Once the fix is plotted, the navigator must assess if the course is following the desired track. This is analogous to a check-reading task where the navigator checks the plotted fix to ensure it is within tolerable limits of the desired track.<sup>33</sup>

Given that the error in the course is detected, the conning officer must ascertain the correct course change to order. This can be as simple as a rudder order. While there is no written procedure to follow, it is assumed that when a course deviation is detected the procedure is to order a course change. The corresponding HEP is taken from "Estimated Probabilities of Error When Using Written Procedures Correctly."

Once the order to change course is given, the helm must properly respond to the order. This involves turning the wheel while watching the rudder angle indicator and the gyro repeater until the ordered course is achieved. The helmsman must immediately respond and the procedure followed involves some skill. The standard order to the helm involves both a rudder angle order and a final course to steady on. The table "Estimated Probabilities of Errors in Recalling Special Instruction Items Given Orally" is used.

**Table 6 - 5: HEPs for Piloting**

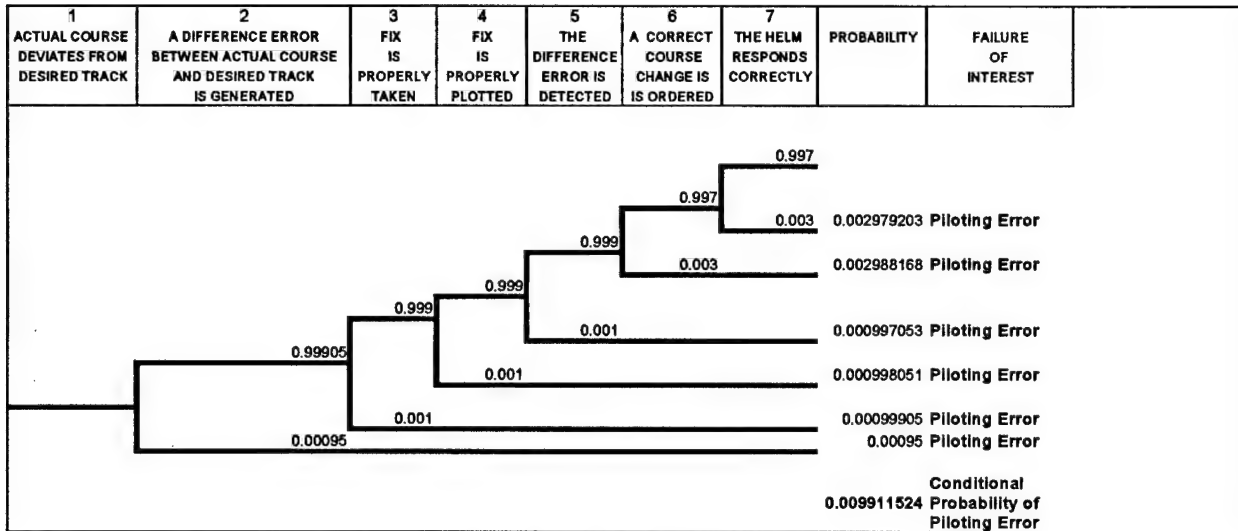
Event Number	Maritime Task	Analogous Nuclear Power Task	HEP	Uncertainty
3	Read radar ranges (take a fix)	Reading a digital display	0.001	0.0005 - 0.005
4	Plot ranges	Recording readings	0.001	0.0005 - 0.005
5	Detect the difference error between actual course and desired track	Check-reading with limits	0.001	0.0005 - 0.005
6	Order a course change	Nonpassive task error of commission	0.003	0.001 - 0.01
7	Helm responds to order	Failure to recall two items given orally	0.003	0.001 - 0.01

Once the helm responds to the order, the next event is to detect that the difference error is eliminated, which begins the sequence of events again. Therefore, the resulting probability is based upon the number of fixes and assumes that the fix frequency is greater than the rate of departure from track.<sup>34</sup>

Figure 6-7 implements the above probabilities in the event tree.

<sup>33</sup> In many restricted waters, the pilotage of a vessel takes on other forms of comparing actual position to desired position, such as visual ranges, parallel indexing, and relative position to a buoy. Singh [52] refers to qualitative estimation and quantitative measurement as the methods mariners use to determine position. For this analysis, it is assumed that the process of computing actual position, regardless of whether there is a qualitative estimation or a quantitative measurement, takes on the HEP for plotting the actual position from a fix.

<sup>34</sup> If the fix frequency was less than the rate of departure from track, then grounding is nearly inevitable since the ship will intersect the hazard before the fix allows an opportunity to determine the *extremus* situation.



**Figure 6 - 7: Piloting Event Tree with Associated Probabilities**

The resulting failure probability for piloting is relatively large. However, recovery actions have not been considered.

A more detailed analysis must be done to determine the failure probability when recovery and redundancy are applied. Considering a verification role for the mate and pilot in taking fixes and ordering course changes upon each other and the helm, the failure probability is lowered. The analogous role in a nuclear power plant is that of either a second checker or an inspector. Table 6-6 summarizes the events and probabilities that are added to incorporate a checking role in Figure 6-8.

**Table 6 - 6: HEPs for Verification Role**

Event Number	Maritime Task	Analogous Nuclear Power Task	HEP	Uncertainty
5	Fix is verified	Hands-on type of checking	0.01	0.005 - 0.05
8	Course is verified	Hands-on type of checking	0.01	0.005 - 0.05
10	Helm response is verified	Hands-on type of checking	0.01	0.005 - 0.05

The process of actively verifying the helm reduces the probability of the helm making an error. From reference [58], the probability of recalling one or more instructions if a supervisor checks to see that the task was done is negligible. For this analysis, negligible will be interpreted as  $10^{-4}$ .

Incorporating the verification role for the mate and the conning officer yields a probability of piloting error of  $2.98 \times 10^{-3}$  shown in Figure 6-8.



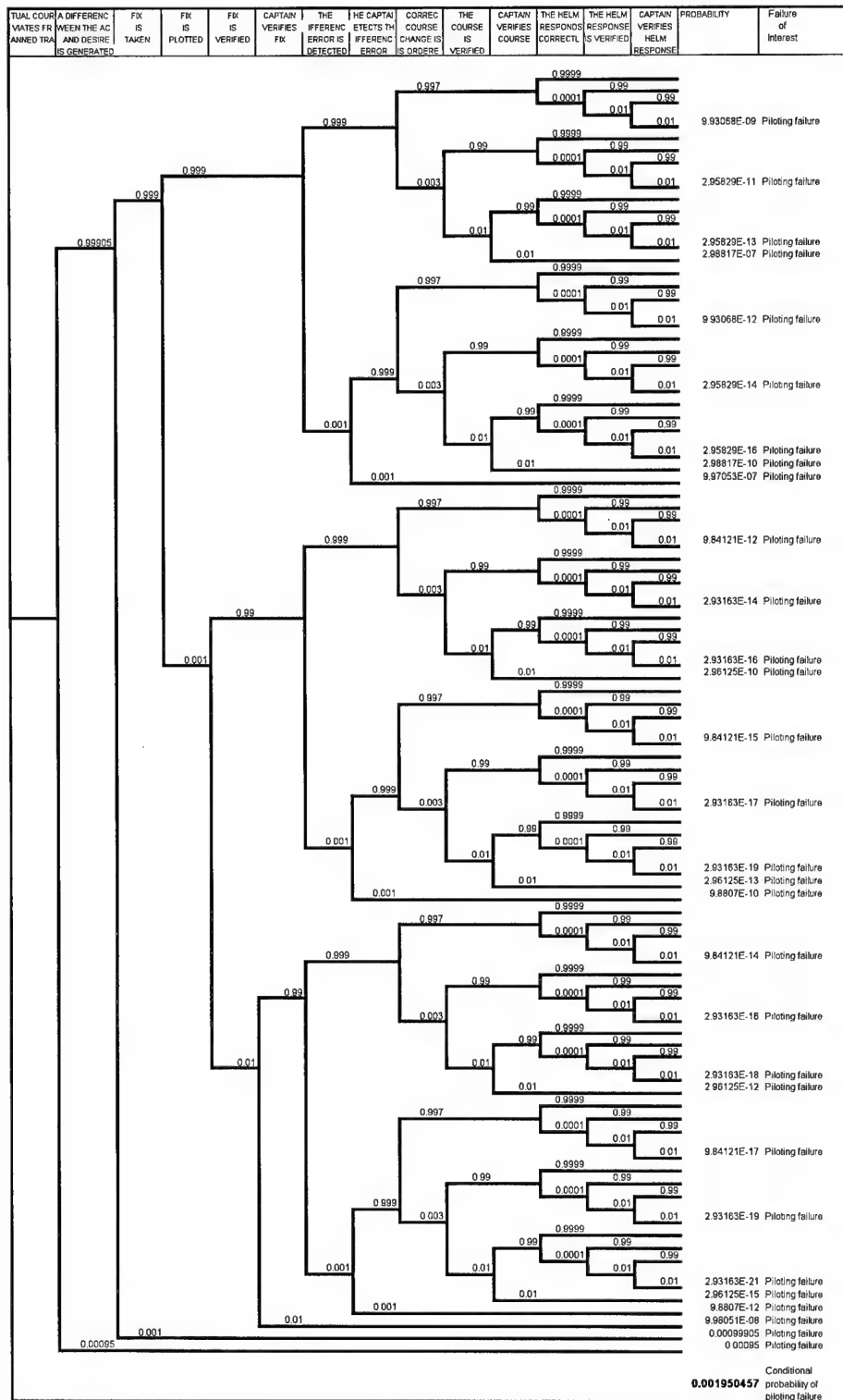


Figure 6 - 9: Piloting Event Tree Incorporating Captains Verification Role

Figures 6-7 through 6-9 show how important the verification role is for each of the officers on the bridge. A summary of the results for the piloting event tree analysis is provided in Table 6-7 for the varying levels of verification:

**Table 6 - 7: Summary of Piloting Failure Probabilities for Varying Levels of Verification**

Level of Verification	Failure Probability
None	$1.38 \times 10^{-2}$
Mate and Conning Officer	$2.98 \times 10^{-3}$
Mate, Conning Officer and Captain	$1.95 \times 10^{-3}$

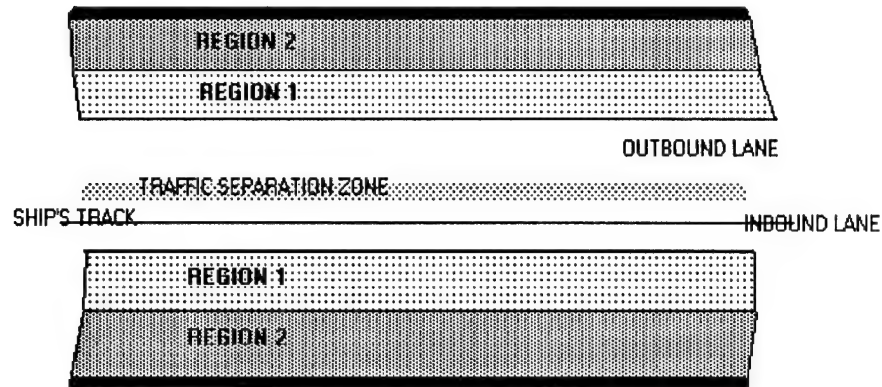
The results show that the additional verification role reduces the failure probability by an order of magnitude. Since the Captain is the individual that is responsible for the vessel, prudence dictates a verification role because it provides an additional recovery event for failure of either the mate or conning officer to perform their respective verification events. The Captain's verification role reduces the failure probability another 30 percent. The Captain plays an integral role in the error detection cycle that will be modeled to allow for a recovery event after each of the piloting processes. The failure probability value of  $1.95 \times 10^{-3}$  will be used for further analysis.

The piloting failure probability is time dependent; as the piloting process is periodic throughout the transit. Additionally, consideration must be made for recovery events after each of the piloting processes as the vessel transits the waterway.

Consider the hypothetical waterway in Figure 6-10. The figure shows the ship's track for an inbound transit. As the ship proceeds down the intended track, there can be errors in the piloting cycle that are not detected, however the ship is not necessarily in a failure state. As the ship deviates from its intended track into Region 1, there exists the ability to recover. Once the ship enters Region 2, however, the ability to maneuver the ship to avoid grounding becomes impossible.<sup>35</sup>

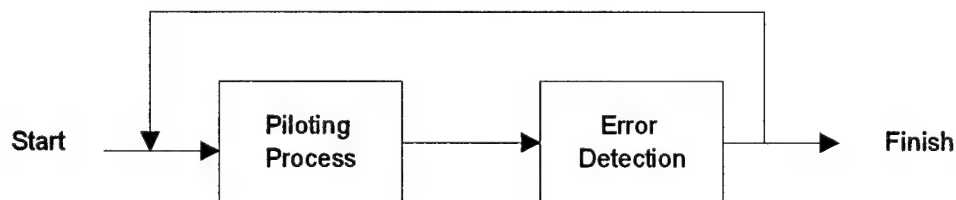
<sup>35</sup> Recall that collision is not considered.

**Region 1: Region for possible recovery**  
**Region 2: Region for no recovery**



**Figure 6 - 10: Hypothetical Waterway**

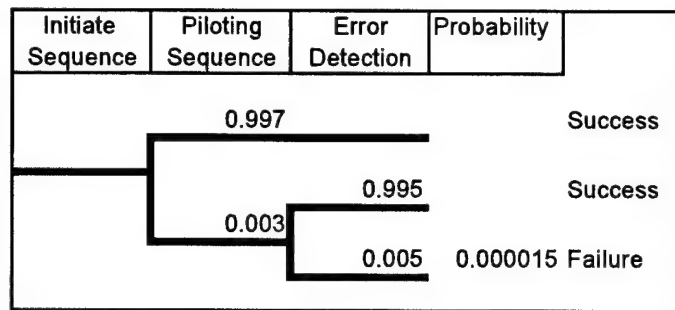
After each sequence of events in the piloting process, there is some probability, given the ship fails to correct its course to the desired track, that the crew will recognize the error and implement correction in the next piloting sequence. Define the error detection factor as the probability that the bridge team will recognize its failure in the piloting cycle before reaching Region 2.



**Figure 6 - 11: Piloting with Recovery Flow Path**

The error detection rate can reflect the attributes of the waterway that the vessel is transiting. Consideration of traffic density, navigational aids, the existence of a Vessel Traffic Service (VTS), the quality of the VTS, the geography of the surrounding land, and the contour of the waterway bottom can all influence the error detection factor and the piloting process. For simplicity, it is assumed that the proximity of the planned track to a shoal has the largest impact, and that impact can be captured in the error detection factor. Therefore, the error detection factor is path dependent. As a result, this value becomes the most subjective value used in this analysis.

From reference [58], the nominal checking probability provides the basis for determining a value for the error detection factor. The lower limit is chosen as the error factor because of the many cues available to the mariner to recover. Given this failure probability, the event tree (Figure 6-12) is constructed from the flow chart of Figure 6-11.



**Figure 6 - 12: Piloting and Recovery Event Tree**

Implicit in the above model, is that the probabilities remain constant through each successive cycle. This is questionable, because as the bridge team fails on one cycle, it is plausible that the likelihood for failure on the next cycle is higher. However, without any data it is difficult to predict. Additionally, the model presumes a path dependent error detection factor. For this analysis, the error detection factor is held constant.<sup>36</sup> This is done for purposes of illustrating the analytic method, and recognizing that further elaboration would be unjustified in the face of poor data.

The resulting probability of piloting failure is an error rate that is the product of the piloting error and recovery factor.

$$\begin{aligned}
 P(\text{piloting failure rate}) &= P(\text{piloting error}) \text{ per piloting cycle} \times \text{Error Detection} & (6-9) \\
 &= 0.00198 \text{ per piloting cycle} \times 0.005 \\
 &= 9.90 \times 10^{-6} \text{ per piloting cycle}
 \end{aligned}$$

$$\text{Piloting cycle} = 3 \text{ minutes}$$

$$P(\text{piloting failure rate}) = 3.3 \times 10^{-6} \text{ per minute}$$

For time dependent functions, the probability of failure of the system as a function of time can be defined by the unreliability function  $F(t)$ . The unreliability function is determined by integrating the probability density function (pdf)  $f(t)$ , which characterizes the behavior of the system.

The exponential distribution used to describe a pdf is given as follows:

$$f(t) = \lambda e^{(-\lambda t)} \quad (6-10)$$

$$\lambda = \text{rate of failure} = \text{the probability that the system will fail between } t \text{ and } t + \Delta \quad (6-11)$$

The hazard rate  $h(t)$  is the probability of the first and only failure of an item in the next instant of time, given that the item is presently operating. One of the characteristics of an exponential distribution is the constant hazard rate with time:

<sup>36</sup> Conceptually, the waterway can be broken down into regions. Each of the regions proximity to a shoal is reflected in the error detection factor. For this analysis, the waterway is considered one continuous region.



$$h(t) = \lambda \quad (6-12)$$

Let the piloting failure rate be represented by the rate of failure  $\lambda$ . Then the unreliability function is determined as follows:

$$F(t) = \int_0^t h(\theta) d(\theta) \quad (6-13)$$

$$F(t) = 1 - e^{(-\lambda t)} \quad (6-14)$$

The probability of piloting failure is now given as  $F(t)$ . The probability of piloting failure along the track is determined by evaluating  $F(t)$  at the time of interest. The behavior of the unreliability over time is shown in Figure 6-13.

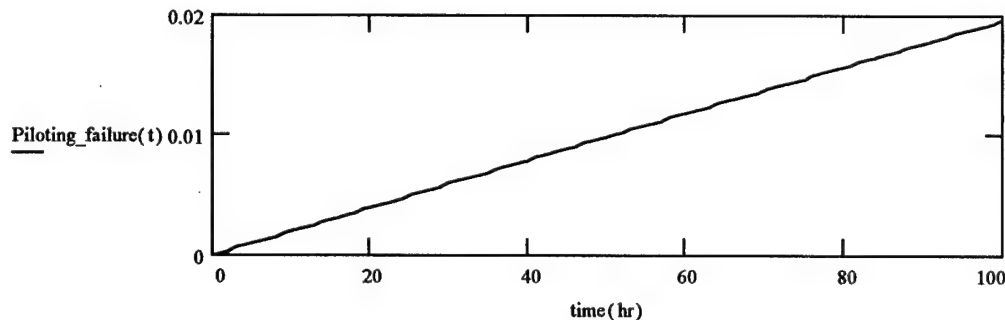


Figure 6 - 13: Piloting Unreliability versus Time

### 6.3 Drift Grounding

The drift grounding portion of the grounding fault tree is shown in Figure 6-14. In order for a drift grounding to occur, all of the failure conditions must be present:

1. *Unsafe wind/current*: the prevailing winds and currents must be such that the environmental forces exerted on the vessel tend the vessel towards an grounding hazard.
2. *Assistance failure*: there is either a failure to request assistance or the assistance fails to tend the vessel away from a grounding hazard.
3. *Anchor failure*: there is failure to let-go the anchor or a failure of the anchor in preventing the vessel from tending towards a grounding hazard.

4. *Loss of steerage way*: the ship is unable to proceed with directional stability due to either a loss of steering or propulsion.

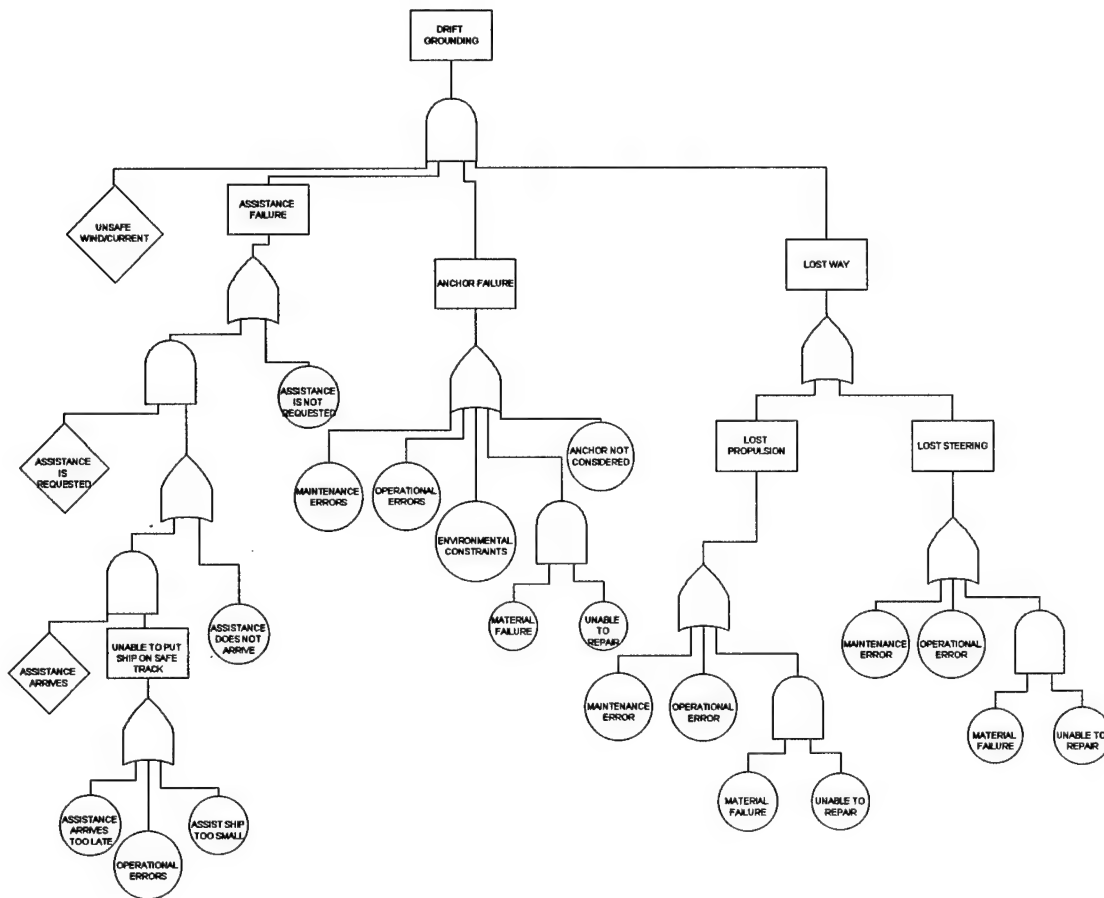


Figure 6 - 14: Drift Grounding Fault Tree

### 6.3.1 Wind and Current

In order to assess the wind and current issues, there must be an analysis of the prevailing winds and currents in the area of concern. This data is dependent upon location. For this analysis, the probability will conservatively be assumed to be 1.0. That is, the wind and current are such to always force a drifting vessel towards a shoal.

### 6.3.2 Rescue and Assistance

Salvage, in its most immediate form, consists of assistance rendered to a vessel that has suffered a casualty and is unable to continue by its own efforts [13]. Traditionally, the size of the salvage market has been dependent upon the size and age of the world fleet [13]. How-

ever, public sensitivity towards pollution and the threat posed by oil tankers have introduced other factors into the salvage market. The salvage industry has been subjected to rising operational costs, growing competition, and static revenue. As a result, the worldwide spread of salvage hardware is patchy [13], leaving a questionable availability in some areas should a crisis occur.

Under the 1989 International Convention on Salvage, the 1990 International Convention on Oil Pollution Preparedness, Response and Cooperation, and OPA 90, greater emphasis is placed on dealing with the problem of pollution prevention.

Currently, few dedicated tugs exist worldwide for these purposes [66]. In most areas, the industry is constrained by a system that relies upon "tugs of opportunity" to provide assistance. This system is bounded by the availability, capability, and expertise of the tugs within a response area [66]. To address the system constraints, there is a momentum towards legislating dedicated rescue tugs and/or escort tugs.

The primary mission of a rescue or escort tug is to provide emergency rescue services for disabled tankers. The objective is to prevent oil spills from disabled tankers that are in imminent danger of grounding. Escort vessels can be the last line of defense in preventing a tanker spill accident resulting from either a loss of power or steering.

The fundamental event tree for a ship requiring assistance is as follows:

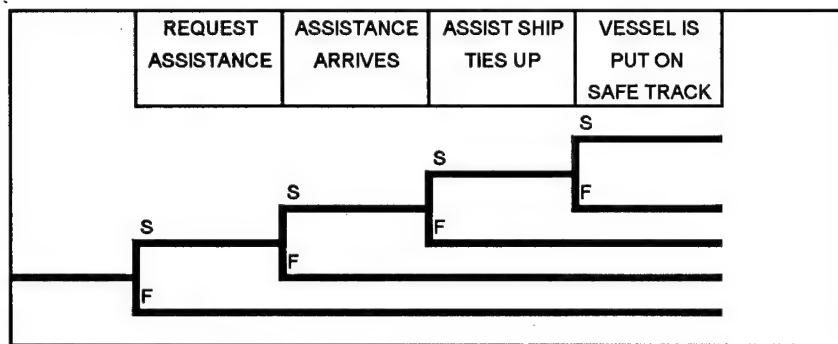


Figure 6 - 15: Assistance Event Tree

Probably the largest contribution to an assistance failure, is the failure to request assistance in time. Once the bridge team recognizes that assistance is required, the stress level is extremely high. History has shown that captains will take calculated risks by delaying contacting assistance in hope of remedying the situation with organic assets. Well known accidents such as the *Amoco Cadiz* and the *Transhuron* typify the concerns of many captains when faced with a situation in which they perceive the receipt of a "bad mark" if they call for assistance when the possibility of restoring the ship to a safe condition still exists in their minds.

Reference [58] documents the probability of error for extremely high stress as being 0.25. Since the resource are not available to determine the probability for assistance arriving and tying up correctly, the 0.25 value will be used.

Currently, escort tugs are required for loaded tankers in Prince William Sound, Puget Sound and San Francisco Bay. Escort by means of a tug tethered to the stern of a tanker to permit rapid response to a steering or propulsion casualty is the typical implementation of the

escort legislation [27]. The preventive measure of having a suitable tug tied to the stern of a tanker removes the system boundaries of availability and capability. The event tree reduces to the probability of the escort tug being able to keep the tanker on a safe track.

The application of escort tugs is for restricted waters. For approaches to restricted waters, tankers do not have an escort. To address the issues of availability and capability, some regions have implemented a dedicated rescue tug. A dedicated rescue tug remains on station in the area of concern. By being on station, the tug is always available. It is able to respond to a tanker in distress within a reasonable time frame.

A study by Robert Allan Ltd. [47] has been done to try to estimate the effectiveness of escort tugs in preventing accidents. The study surveyed casualty databases of Canada and the U.S. to determine accidents involving the interaction of tugs with ships greater than 5,000 gross tons and tugs. Utilizing the accident quotient to approximate the failure probability:

$$\text{Accident Quotient} = \frac{\text{Number of Groundings}}{\text{Number of Vessel Movements}} \quad (6-15)$$

The following table summarizes the results of reference [47] which resulted in groundings to determine the accident quotients:

**Table 6 - 8: Tanker-Tug Grounding Accidents**

Area	Approximate Number of Vessel Movements	Number of Groundings	Accident Quotient
Strait of Jan de Fuca	500,000	2	$4.0 \times 10^{-6}$
St. Lawrence River	100,000	5	$5.0 \times 10^{-5}$
Bay of Fundy	60,000	6	$1.0 \times 10^{-4}$
<b>Channel Weighted Mean</b>			<b><math>5.1 \times 10^{-5}</math></b>
<b>Standard Deviation</b>			<b><math>4.8 \times 10^{-5}</math></b>

From the above table, the failure of a dedicated escort tug in preventing a grounding is assumed to be  $5.0 \times 10^{-5}$ .

Based upon the limited analysis done above, the differences in the probability of an assistance failure varies from  $2.5 \times 10^{-1}$  without dedicated rescue tugs to  $5.0 \times 10^{-5}$  with dedicated rescue tugs.

### 6.3.3 Anchor Failure

Tankers will have two anchors. Anchors on large tankers can weigh as much as 50,000 pounds each. Unfortunately, as ships have gotten larger, the proportionate sizes of anchors have decreased. The ratio of the anchor weight to the deadweight tonnage has dwindled from about 0.6 to 0.2 [7]. The anchors of large tankers are suitable for anchorage in designated areas, but with any significant way on the ship when dropping anchor, the momentum can become too great for the anchor system. According to reference [11], for a large vessel, speed is

the most significant factor to consider if an anchor system is used to stop the ship. DNV [11] concludes that at speeds greater than 1 knot, the anchor system will fail if it is deployed.

It is difficult to ascertain any valid statistical data relating to anchor failure. A query of the CASMAIN database reveals 58 vessel casualty reports between the years 1981 and 1991 where a cause was attributable to a dragging anchor. This represents less than 0.1 percent of all the vessel casualties recorded. Of these 58 vessels, only 12 are tankers. The nature of the query limits causality to post letting-go anchor failure, where the nature of the failure can be attributed to unfavorable environmental constraints.

An additional query of ground-tackle material failure revealed another 15 tanker accident reports. These failures give an indication of the material failure rate of tanker anchor system.

It is impossible to assign any failure data to either maintenance or operational errors. Based upon 4 of the total 27 tanker accidents, attributed to some form of failure of the anchor system, which took place in the New Orleans/Baton Rouge waterway over the 11 year coverage of the CASMAIN database, a rough order of magnitude estimate of anchor failure rate is assumed. The average number of tanker trips in the New Orleans/Baton Rouge waterway over the years 1986-1990 was 2,765 trips. If this average is assumed for the 11 years for which the database covers, a total of 30,415 trips results. If this value is divided into the 4 anchor failure accidents occurring in this waterway, then an accident quotient of  $1.3 \times 10^{-4}$  results.

$$\text{Anchor Failure Accident Quotient} = \frac{\text{Number of Anchor Failures}}{\text{Number of Transits}} \quad (6-16)$$

Table 6 - 9: Anchor Failure Accident Quotient

Total Assumed Tanker Transits for New Orleans/Baton Rouge (1981 through 1991)	Number of Anchor Failures	Accident Quotient
30,415	4	$1.315 \times 10^{-4}$

Based upon the above accident quotient, the probability of anchor failure will be assumed to be  $1.3 \times 10^{-4}$ . This estimate is quite conservative, and based solely on the traffic within the New Orleans/Baton Rouge waterway.

Unfortunately, it is nearly impossible to extract from the database those cases where an accident occurred because the anchor was not considered. The grounding of the *Braer* is clear example where consideration for dropping the anchor could have significantly impacted the results of that tragedy. Because accidents do occur as a result of failing to consider the anchor, a failure probability needs to be assigned to this basic fault.

Failure to consider dropping the anchor is a failure related to administrative control in reference [58]. This refers to the organizational structure, both real and perceived, that motivates the operator to make the right decisions and to follow policy and procedures. The situation that may require dropping the anchor is stressful. Based on an extremely high stress level, an HEP of 0.25 is assigned to this basic fault.

The probability of an anchor failure is dominated by the HEP of 0.25 for considering the anchor in time to be effective. Therefore, the probability for anchor failure is considered to be 0.25.

### 6.3.4 Lost Way

The loss of way is broken down into two categories: loss of propulsion, and loss of steering. Like the operations on the bridge, many of the failures related to loss of propulsion and loss of steering can be traced to human failure and individual error. Time precludes performing a detailed analysis of the engineering plants, yet this is an area that warrants further investigation. On a recent tanker visit, the engineering department was provided with neither operating, nor casualty procedures.

Figure 6-16 shows the number of lost way incident per year from 1981 through 1991.<sup>37</sup>

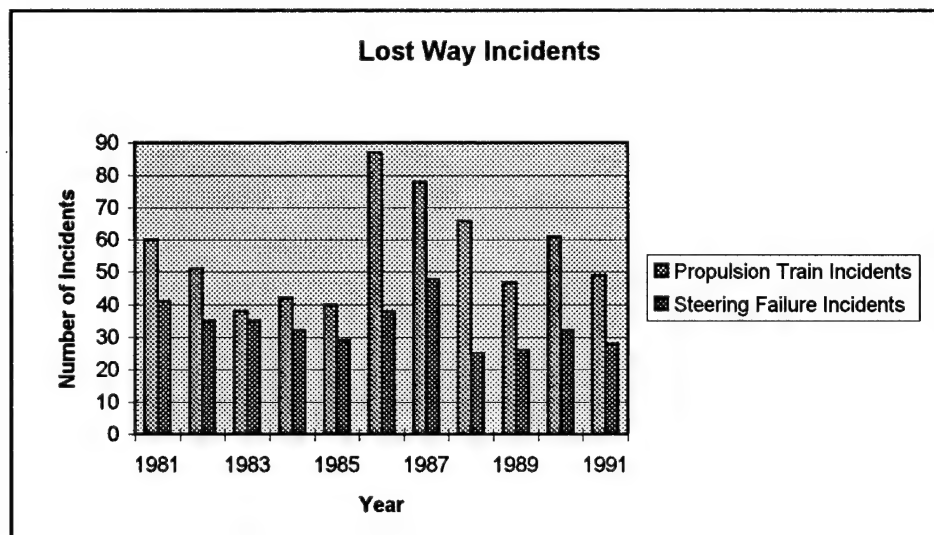


Figure 6 - 16: Tanker Lost Way Incidents (1981-1991)

<sup>37</sup> Based on a search of the CASMAIN database, the results show all steering failures and propulsion train incidents include material failure of:

1. Main Engines
2. Boiler
3. Main Steam System
4. Feed and Condensate System
5. Fuel Oil Supply
6. Lube Oil Supply
7. Main Generator
8. Reduction Gear
9. Shaft System
10. Propeller

In order to estimate the probability of a loss of way incident, the number of incidents over a given time period is compared to the number of tanker transits. Table 6-10 summarizes the results.

$$\text{Lost Way Accident Quotient} = \frac{\text{Number of Lost Way Incidents}}{\text{Number of Transits}} \quad (6-17)$$

**Table 6 - 10: Lost Way Accident Quotients**

Port	Tanker Transits	Propulsion Failures	Propulsion Failure Accident Quotient	Steering Failures	Steering Failure Accident Quotient
Valdez	8708	5	$5.74 \times 10^{-4}$	1	$1.15 \times 10^{-4}$
San Francisco Bay	10,133	3	$2.96 \times 10^{-4}$	1	$9.87 \times 10^{-5}$
New Orleans/Baton Rouge	13,825	28	$2.03 \times 10^{-4}$	12	$8.68 \times 10^{-4}$
<b>Total</b>	<b>32,666</b>	<b>36</b>	<b><math>1.10 \times 10^{-3}</math></b>	<b>14</b>	<b><math>4.29 \times 10^{-4}</math></b>

Since the failure rate is dependent upon the transit length, a rough estimate of the near-land transit length for each port is included in the following table:

**Table 6 - 11: Approximate Coastal Transit Length (miles)**

Port	Approximate Transit Miles
Valdez	100
San Francisco Bay	40
New Orleans/Baton Rouge	200

The aggregate failure probabilities are divided by the total number of transit miles of 340 mi. to approximate the failure probability per mile.

**Table 6 - 12: Lost Way Failures per Mile**

Propulsion Failure Probability	Steering Failure Probability	Propulsion Failures per Mile	Steering Failures per Mile
$1.1 \times 10^{-3}$	$4.29 \times 10^{-3}$	$3.24 \times 10^{-6}$	$1.26 \times 10^{-5}$

The probability per mile of having a loss of way accident becomes the sum of the two probabilities (assuming independence and the rare event approximation). Therefore, the probability of having a loss of way accident becomes  $4.5 \times 10^{-6}$  per mile. If this is multiplied by the ships speed to put it into a function of time, the value can be considered a constant hazard rate function.

Recall:

$$f(t) = \lambda e^{(-\lambda t)} \quad (6-18)$$

$\lambda$  = rate of failure = the probability that the system will fail between  $t$  and  $t + \Delta$  (6-19)

Let the rate of failure be equal to the probability per mil times the speed of the ship.

$$\begin{aligned} s &= \text{speed} \\ \lambda &= \text{rate of failure} = 4.5^{-6} s \\ h(t) &= \lambda = 4.5^{-6} s \end{aligned} \quad (6-20)$$

$$F(t) = \int_0^t f(e) d(e) \quad (6-21)$$

$$F(t) = 1 - e^{(-\lambda t)} = 1 - e^{-0.0000045st} \quad (6-22)$$

The behavior of the unreliability over time (assuming 10 kts) is as follows:

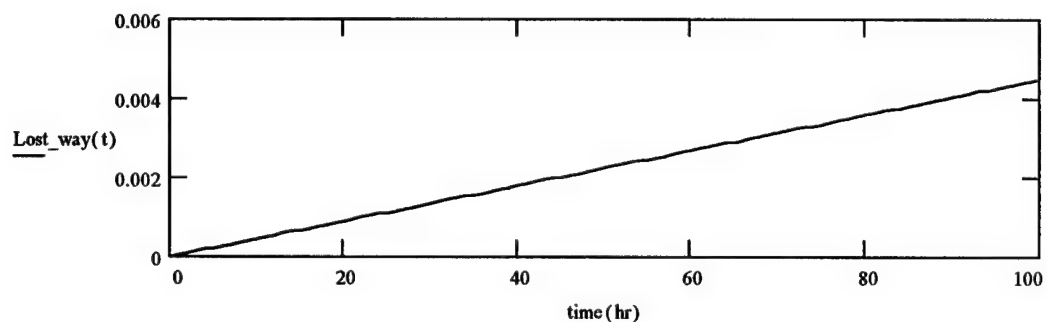


Figure 6 - 17: Lost Way Unreliability versus Time

## 6.4 Summary of Probabilities

The probabilities that were determined from both event trees and historical data are summarized in the Table 6-11.

To evaluate the overall probability of grounding the powered grounding and drift grounding fault trees will be reduced to incorporate the above values.



**Table 6 - 13: Summary of Grounding Probabilities**

<b>Powered Grounding:</b>	
Faulty Passage Plan	$7.005 \times 10^{-5}$
Faulty Planning Information	$1.0 \times 10^{-4}$
Piloting Error	$1 - e^{-0.0000033t}$
<b>Drift Grounding:</b>	
Sufficient Wind/Current	1
Assistance Failure	0.25
Anchor Failure	0.25
Lost Way:	$1 - e^{-0.0000045st}$

## 6.5 Fault Tree Reduction

The grounding fault tree has been inductively and deductively constructed for clarity in order to determine the basic faults of grounding accidents. Because the basic faults have now been identified, reduction of the fault tree will make the connection between the probabilities and the fault tree clearer. By incorporating Boolean identities, the fault tree can be reduced to a simpler expression.

### 6.5.1 Powered Grounding Fault Tree Reduction

From Figure 6-2, the Boolean expression for powered grounding is:

$$P(\text{powered grounding}) = P(\text{desired track is unsafe}) + P(\text{course deviates from safe desired track}) \quad (6-23)$$

$$P(\text{desired track is unsafe}) = P(\text{errors made in planning track}) + (P(\text{no errors made in planning track}) * P(\text{planning information is not accurate})) \quad (6-24)$$

$$P(\text{course deviates from safe desired track}) = P(\text{difference error is not detected}) + (P(\text{difference error is detected}) * P(\text{insufficient action to eliminate the error})) \quad (6-25)$$

By recognizing the  $P(\text{errors made in planning track})$  is the negation of  $P(\text{no errors in planning track})$  in equation (6-24), and likewise for the  $P(\text{difference error is detected})$  and  $P(\text{difference error is not detected})$  in equation (6-25), then equations (6-24) and (6-25) reduce through Boolean identities to the following:

$$P(\text{desired track is unsafe}) = P(\text{errors made in planning track}) + P(\text{planning information is not accurate}) \quad (6-26)$$

$$\begin{aligned}
 P(\text{course deviates from safe desired track}) = & \\
 & P(\text{difference error is not detected}) \\
 & + P(\text{insufficient action to eliminate the error}) \quad (6-27)
 \end{aligned}$$

The piloting event tree incorporates all of the information contained in Equation (6-27). Rather than dissect the event tree, it is easier to equate the results of the event tree to the probability of the course deviating from a safe desired track. Therefore:

$$P(\text{course deviates from safe desired track}) = P(\text{piloting error}) \quad (6-28)$$

Utilizing the reductions, the expression for the probability of a powered grounding is:

$$\begin{aligned}
 P(\text{powered grounding}) = & P(\text{errors made in planning track}) \\
 & + P(\text{planning information is not accurate}) \\
 & + P(\text{piloting error}) \quad (6-29)
 \end{aligned}$$

By assuming independence and the rare event approximation, the above Boolean expression becomes the sum of the probabilities.

$$P(\text{powered grounding}) = 7.005 \times 10^{-5} + 1.0 \times 10^{-4} + (1 - e^{-0.0000033t}) \quad (6-30)$$

## 6.5.2 Drift Grounding Fault Tree Reduction

The fault tree for drift grounding is shown in Figure 6-14. The methodology used to determine the probabilities for the elements of drift grounding limits the values to estimates that represent the first level of the drift grounding fault tree:

$$\begin{aligned}
 P(\text{drift grounding}) = & P(\text{unsafe wind/current}) \\
 & * P(\text{assistance failure}) \\
 & * P(\text{anchor failure}) \\
 & * P(\text{lost way}) \quad (6-31)
 \end{aligned}$$

The probability of lost way is the only term broken down to another level:

$$\begin{aligned}
 P(\text{drift grounding}) = & P(\text{unsafe wind/current}) \\
 & * P(\text{assistance failure}) \\
 & * P(\text{anchor failure}) \\
 & * (P(\text{lost propulsion}) + (P(\text{lost steering}))) \quad (6-32)
 \end{aligned}$$

Again, by assuming independence and the rare event approximation, the probability for drift grounding becomes an expression of products:

$$P(\text{drift grounding}) = 1.0 \times 0.25 \times 0.25 \times (1 - e^{-0.0000045t}) \quad (6-33)$$

## 6.6 The Probability of Grounding

The probability of grounding is approximated as the sum the probabilities for drift grounding and powered grounding:

$$\begin{aligned} P(\text{grounding}) &= P(\text{powered grounding}) + P(\text{drift grounding}) \\ &= 1.7 \times 10^{-4} + (1 - e^{-0.0000033t}) + ((6.25 \times 10^{-2}) \times (1 - e^{-0.0000045st})) \end{aligned} \quad (6-34)$$

Figure 6-18 graphs the powered grounding, drift grounding, and the grounding probabilities against time. From this figure it can be seen that powered grounding dominates the contribution to the probability of grounding.

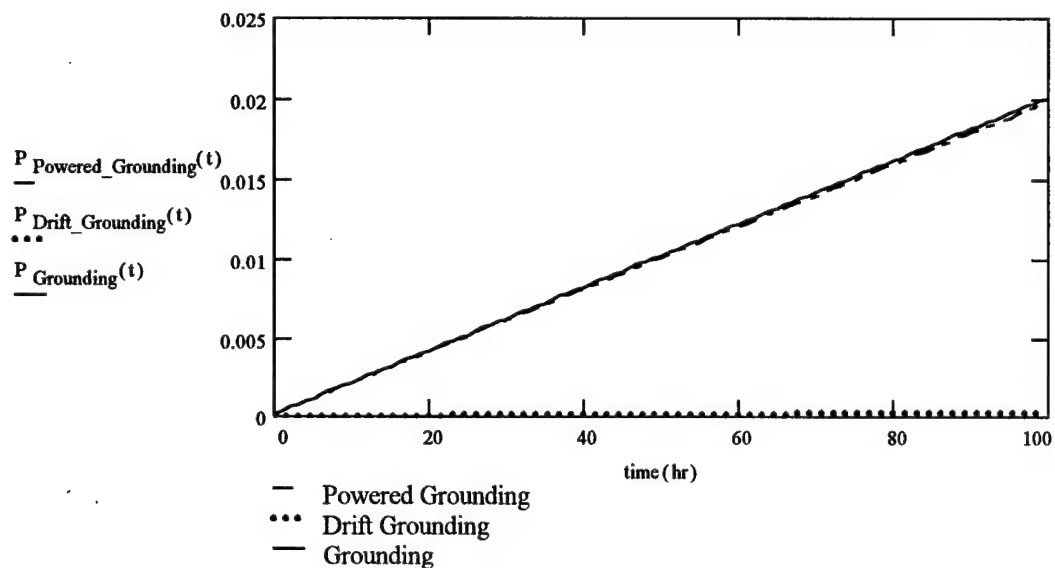


Figure 6 - 18: Grounding Probabilities with Time

## 6.7 Summary

The resulting probability for grounding is dominated by the piloting process in the powered grounding mode of failure. This is confirmed by the CASMAIN database, which attributes only 15 cases of 716 tanker groundings to either steering failure, or propulsion failure. This analysis seems to overestimate the probability of powered grounding based upon statistical data. However, mariners tend to operate by allowing large margins for error, it may be that errors occur, but the allowed margins mitigate any adverse consequences. At the same time,

continuous errors in these margins do not provide sufficient feedback to the mariner. As a result, the wrong behavior is repeated until the margin no longer exists to impede the inevitable adverse consequences.

The method to determine the probability of powered grounding, while simplistic, is systematic. Because each of the processes are broken into a sequence of events, a sensitivity analysis of each event over the range of uncertainty can show those areas where the greatest potential for reducing the probability of grounding exists. Likewise, those areas can be identified that produce the greatest potential for the increase in grounding probability. Once identified, policy makers are able to make rational decisions regarding the allocation of limited resources to reduce the possibility of grounding and ultimately minimize the outflow of oil into the environment.

## Chapter 7 Evaluations and Conclusions

### 7.1 High-Leverage Factors

In order to determine those events that offer the largest potential for improving the failure probabilities requires a sensitivity analysis. Once performed, the high-leverage factors can identify risk reduction areas, and resources allocated to promote reducing the probability of grounding, or at least to implement measures to prevent increasing the probability. For the grounding event, powered grounding is shown to be the significant contributor. A sensitivity analysis of the event trees incorporated in the powered grounding analysis identifies the high-leverage factors.

### 7.2 Powered Grounding Sensitivity Analysis

Recall that the three major elements for determining the probability of powered grounding are: planning, planning information, and piloting. The high-leverage factors are determined by varying each of the probability events in the event tree over the range of uncertainty. The results of the sensitivity analysis are displayed in Appendix D. The following paragraphs summarize a sensitivity analysis to determine which factors within these elements warrant further consideration

#### 7.2.1 Planning Failure Sensitivity

The sensitivity analysis of the planning event tree yields three events that can significantly affect the probability for implementing a faulty plan. Recall that the event tree analysis resulted in a mean probability for implementing a faulty plan of  $7.005 \times 10^{-4}$ . The effect of each high-leverage event on the probability for implementing a faulty plan at the low-end and high-end of the uncertainty is summarized in Table 7-1.

**Table 7 - 1: Planning Failure Event Tree High-Leverage Factors**

Event	Percent Deviation from the Mean Probability at the Low-End of Uncertainty	Percent Deviation from the Mean Probability at the High-End of Uncertainty
check publications for changes	-28%	100%
determine waypoints	-28%	100%
captain verify plan	-50%	4900%

From Table 7-1 it can be seen that the events that offer the largest improvement are:

1. Captain's verification.
2. Checking publications for changes in the waterway.
3. Properly determining the voyage waypoints.

For voyage planning, it is essential to begin with the correct information by checking publications, incorporating the changes on the charts, and determining the correct waypoints. The most important event is that of verification. The captain's verification event has an impact on the complete planning process.

While these factors offer the greatest potential for improvement, over the range of uncertainty, they offer a greater potential for increasing the probability of failure. This emphasizes the importance of navigation fundamentals and the captain's role in verifying that the track meets imposed constraints.

When the probability of faulty planning information is included in the sensitivity analysis, Table 7-2 results in the sensitivity for failure to implement a correct track.

**Table 7 - 2: Planning Failure Event Tree (incorporating the probability for faulty information) High-Leverage Factors**

<b>Event</b>	<b>Percent Deviation from the Mean Probability at the Low-End of Uncertainty</b>	<b>Percent Deviation from the Mean Probability at the High-End of Uncertainty</b>
check publications for changes	-12%	41%
determine waypoints	-12%	41%
captain verify plan	-21%	2018%
utilize faulty information	-53%	529%

It can be seen from Table 7-2 that over the range of uncertainty, faulty navigational information offers the greatest potential for improving the failure probability.

## **7.2.2 Piloting Failure Sensitivity**

Table 7-3 shows the affect of the high-leverage piloting events on the overall probability for a piloting failure determined from the event tree that incorporates the captain's verification role.

**Table 7 - 3: Piloting Failure Event Tree High-Leverage Factors  
(incorporating Captain's verification role)**

<b>Event</b>	<b>Percent Deviation from the Mean Probability at the Low-End of Uncertainty</b>	<b>Percent Deviation from the Mean Probability at the High-End of Uncertainty</b>
a difference error is generated	-49%	3%
a proper fix is taken	-26%	205%

To gain further insight into the scope of the potential for the high-leverage factors, an additional sensitivity analysis for the event tree that does not incorporate the captain's verification role is considered. The following table summarizes the results.

**Table 7 - 4: Piloting Failure Event Tree High-Leverage Factors  
(without captain's verification role)**

<b>Event</b>	<b>Percent Deviation from the Mean Probability at the Low-End of Uncertainty</b>	<b>Percent Deviation from the Mean Probability at the High-End of Uncertainty</b>
a difference error is generated	-32%	2%
a proper fix is taken	-17%	135%
the difference error is detected	-17%	135%

From the previous two tables it is seen that the most sensitive events are also the most fundamental events to piloting and navigation:

1. Generating a difference error.
2. Properly taking a fix.
3. Detecting a difference error from the plotted fix.

Reductions in piloting error are dominated by the accuracy and reliability of the navigational equipment (a difference error is generated) and fundamental piloting techniques (fix is taken and a difference error is detected). Regardless of any verification processes, if these fundamental events fail, then there is a significantly higher probability of failure. The sensitivity analysis captures the fact that a lot of coastal piloting is done by experience and line-of-sight piloting, rather than actual plotting. Therefore, regardless of the methods used to determine the ship's position, if the conning officer is unable to detect that the ship has deviated from the desired track then the potential for grounding increases.

## 7.3 Recommendations

The results of the sensitivity analysis identifies those high-leverage factors that have potential for impacting the probability for powered grounding:

1. *Planning*: Check publications for changes  
Determine waypoints properly  
Captain Verify Plan
2. *Planning Information*
3. *Piloting*: Difference error is generated  
Take fixes properly  
Difference error is detected

The salient question remains: "What measures will effectively and efficiently influence the high-leverage factors to reduce the probability of grounding?"

Recall that the constituents of human failure are:

1. Sub-systems.
2. Procedures.
3. Organizations.
4. Environment.
5. Individuals.

### 7.3.1 Sub-System Improvements

Within the confines of sub-systems there is a technology that can promote a reduced probability for powered grounding. Recall however, that the implementation of technology, alone, does not result in a reduced failure rate. Because the technology must interface with the individual, the technology must be implemented without increasing the complexity of the system, while ensuring that operators understand the technology and its limitations.

The potential for ECDIS, if implemented properly, to reduce planning errors is great. Its implementation can include the automatic update of charts via satellite, process meteorological data, incorporate individual vessel characteristics to plan voyages and optimize those voyages for either time or fuel considerations. It must be recognized though, that the output is only as good as its input, and the National Oceanic and Atmosphere Administration (NOAA)



has neither the plans nor the money to implement an updated survey program for the coastal waterways of the U.S.<sup>38</sup>

The potential for ECDIS to improve the piloting error in coastal waterways is also significant. If properly integrated with Differential GPS, it can provide automatic warnings to navigational hazards. The use of DGPS can significantly increase the probability of detecting any deviations from a safe track.

The USCG conducted a simulator experiment to evaluate the effectiveness of the mariner's use of ECDIS in a restricted maneuvering situation [9]. The conclusions were that ECDIS increased safety by both decreasing the magnitude of the ship's deviation from the planned track and increasing the proportion of time that the mariner allocated to collision avoidance and looking out for hazardous situations. In general, ECDIS provided the mariner with a greater situational awareness [56]. The contribution of ECDIS to the safety of navigation was confirmed in sea-trial experiments [18].

The integration of ECDIS into the ship's radar system, DGPS, and a satellite link to incorporate the updating of coastal waterways can reduce the probability of powered grounding. This is accomplished by significantly reducing the impact of the high-leverage factors identified in the piloting process.

As a *caveat*, it was found that the effect of a failure of the ECDIS capability of automatically updating the ship's position increased the number and magnitude of deviations from the planned track [9]. Therefore, issues of reliability need to be resolved with possibly the inclusion of redundant systems and prudent secondary means of positioning.<sup>39</sup> A fully integrated system has the potential to present the mariner with too much information and increase the complexity of the navigational task. The interface of the integrated ECDIS system must be designed ergonomically.

### 7.3.2 Organizational and Procedural Improvements

In conjunction with emerging technologies, there must be corresponding attention given to the organizational aspects of utilizing that technology.

The organizational impact on human failure has the potential to be significantly reduced through implementation of the International Safety Management Code (ISM). In a move away from the traditional hardware requirements, the IMO has mandated the ISM to include the human aspects associated with both vessel and shoreside management. The ISM requires vessels to carry a Safety Management Certificate, and operating companies to have a Document of Compliance.<sup>40</sup> Ships will be retained in port for not producing the necessary documents.

As the preamble to the ISM states [23]:

---

<sup>38</sup> Personal conversation, Larue E., USCG. May 3, 1996.

<sup>39</sup> The grounding of the Royal Majesty presents a situation where the satellite positioning system malfunctioned and no one on the bridge was vigilant enough to confirm the vessel's position.

<sup>40</sup> The International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management Code) was adopted by the IMO in 1993. It becomes mandatory for tankers over 500 gross tons in July, 1998.

The cornerstone of good safety management is commitment from the top. In matters of safety and pollution prevention it is the commitment, competence, attitudes and motivation of individuals at all levels that determines the end result.

The ISM offers broad guidelines for implementing a safety management system that incorporates the following objectives [23]:

1. Provide for safe practices in ship operation and safe working environment.
2. Establish safeguards against all identified risks.
3. Continuously improve safety management skills of personnel ashore and board ships, including preparing for emergencies related both to safety and environmental protection.

The intent of the IMO is to provide a framework for a safety management system that will furnish the impetus for better policies and procedures, thereby creating a more suitable environment for the mariner and producing more motivated, knowledgeable, and safer crews. Once risks are identified, ISM provides the tool to successfully manage those risks.

With sensitive natural resources potentially affected by poor management of risk, it is axiomatic that a vessel owner or operator adhere to a management model which minimizes marine environmental risks and ensures compliance with all applicable laws [65].

The existence of a management policy is not sufficient. To be effective, the policy must be active. A study conducted by the UK P&I Club [61] has shown that an active management policy:

1. Reduces the distance between operator and employee.
2. Increases crew loyalty.
3. Improves manning level compliance.
4. Improves manning qualifications.

In general, the an active management policy, such as the ISM, has the potential to increase the understanding of responsibilities and systems; therefore, better performance.

## **7.4 Conclusions**

Tankers are the largest contributor by vessel type to the worldwide oil spill volume and the grounding of tankers represents a significant failure state contributing to the total acciden-

tal oil outflow of tankers. A systematic approach has been undertaken to gain an insight into the factors that contribute to the grounding event. The fault tree/event tree method for determining the probability of grounding has been used to identify the significant basic faults.

The human element in maritime accidents has been shown to be a major contributor. The THERP analysis provides the tool to gain an understanding into the tasks that the mariner performs. From the task analysis, the high-leverage factors are identified.

Recognizing that individual errors are a subset of human failures, which are a subset of system failures, effective reductions in the individual error rate must encompass total systems approach.

While the approach has been simplistic in nature, the methodology is sound and proven in the nuclear industry. Because of the limited resources available some assumptions taken give rise to the validity of the absolute value for the probability of grounding. However, it does serve to give a relative value and indicate areas for improvement.

Specific areas for improvement lie within the domain of sub-systems, the organization and procedures. An integrated ECDIS system seems to offer significant potential to reduce piloting and planning errors, while ISM offers a framework to enhance safety within the maritime industry and provides an impetus to facilitate the flow of information and provide incentives; thereby increased performance. Additional improvements have been shown to be required in the surveying of coastal waterways.

## **7.5 Areas for Further Research**

The task analysis encompassed in the event trees, while systematic, is simplistic due to the nature of the study. A more detailed task analysis in the framework of the event tree approach can give more insight into the piloting task. This research can take the form of simulator experiments in order to capture the HEPs that are particular to the mariner.

Accident investigations tend to invoke stop rules. A study of the essential elements of an investigation, within the framework of a PRA, can allow investigators to collect essential data so that feedback can provide valuable data to assist in identifying areas for risk reduction.

This thesis has concentrated on a level 1 analysis within the proposed risk model. Further work to expand the analysis to levels 2 and 3 can offer the appropriate risk; that is, incorporating the impact of the accident with the probability of the accident.

## Appendix A Boolean Algebra and Probability Theory

### Boolean Algebra

Fault trees graphically show the logical relationship between various faults and the top event. Boolean algebra is an appropriate tool to represent the fault tree in mathematical form in order to facilitate quantitative analysis.

Table A - 1: Laws of Boolean Algebra

$A * B = B * A$ $A + B = B + A$	Commutative Law
$A * (B * C) = (B * C) * A$ $A + (B + C) = (A + B) + C$	Associative Law
$A * (B + C) = A * B + A * C$ $A + B * C = (A + B) * (A + C)$	Distributive Law
$A * A = A$ $A + A = A$	Idempotent Law
$A * \bar{A} = 0$ $A + \bar{A} = 1$	Complementation Law
$A * (A + B) = A$ $A + (A * B) = A$	Absorption Law
$\overline{(A * B)} = \bar{A} + \bar{B}$ $\overline{(A + B)} = \bar{A} * \bar{B}$	DeMorgan's Theorem

### Laws of Probability

Boolean equations can then be evaluated using the laws of probability. The Boolean symbols “+” and “\*” represent the OR and AND operations respectively. These operations respectively correspond to the union and intersection operations.

**Union**

Boolean Expression:

$$C = A + B$$

Probability Expression:  $P(C) = P(A) + P(B) - P(A * B)$ **Intersection**

Boolean Expression

$$C = A * B$$

Probability Expression:

Independent:

$$P(C) = P(A) * P(B)$$

Dependent:

$$P(C) = P(A) * P(B|A)^{41}$$

Probabilities of dependent events can be evaluated using Baye's theorem:

For two events A and B,

$P(A)$  = the probability of event A.

$P(B)$  = the probability of event B.

$P(A|B)$  = the probability of event A given the occurrence of event B.

$P(B|A)$  = the probability of event B given the occurrence of event A.

$P(AB)$  = the probability of event A and B.

Utilizing set theory,  $P(AB)$  is the intersection of the two events:

$P(B/A)$  is concerned with the darkened part of Figure 5 and is the ratio of the area (AB) to the total area A, that is:

$$P(B|A) = \frac{P(A * B)}{P(A)} \quad (1)$$

By symmetry it may be shown that:

$$P(A|B) = \frac{P(AB)}{P(B)} \quad (2)$$

Solving for  $P(A * B)$ :

$$P(A * B) = P(A)P(B|A) = P(B)P(A|B) \quad (3)$$

<sup>41</sup> The notation  $P(A|B)$  denote the dependent probability of event A occurring, given the knowledge that even B has occurred.

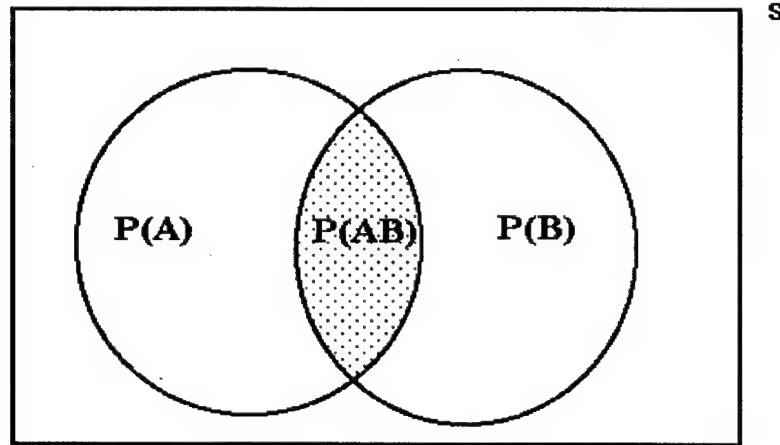


Figure A - 1: Venn Diagram

## Rare Event Approximation

The rare event approximation, also known as the small probability approximation, is applicable when the intersection probability,  $P(A * B)$ , is much smaller than the individual probabilities,  $P(A)$  and  $P(B)$ , generally, 0.1. Utilizing the rare event approximation, the union operation is approximated as follows:

### Union

Boolean Expression:  $C = A + B$

Probability Expression:  $P(C) \cong P(A) + P(B)$

## Generalized Probability Equations

The generalization of the probability equations to  $n$  events is as follows:

### Union

$$\begin{aligned}
 P(A_1 + A_2 + \dots + A_n) = & [P(A_1) + P(A_2) + \dots + P(A_n)] \\
 & - [P(A_1A_2) + P(A_1A_3) + \dots + P_{i \neq j}(A_iA_j)] \\
 & + [P(A_1A_2A_3) + P(A_1A_2A_4) + \dots + P_{i \neq j \neq k}(A_iA_jA_k)] \\
 & \vdots \\
 & (-1)^{n-1} [P(A_1A_2\dots A_n)]
 \end{aligned}$$

Utilizing the rare event approximation:

$$P(A_1 + A_2 + \dots + A_n) \cong P(A_1) + P(A_2) + \dots + P(A_n)$$

**Intersection**

Dependent:

$$P(A_1 A_2 \dots A_n) = P(A_1)P(A_2|A_1)P(A_3|A_1 A_2) \dots P(A_n|A_1 A_2 \dots A_{n-1})$$

Independent:

$$P(A_1 A_2 \dots A_n) = P(A_1)P(A_2) \dots P(A_n)$$

## Appendix B Developing the Grounding Fault Tree

To develop the fault tree for groundings, it must be recognized that a grounding is caused by the ship entering an area where the draft exceeds the depth. It becomes necessary to determine why the ship has encountered that situation. Fundamentally, the ship can either follow a safe track or an unsafe track. An unsafe track necessarily intersects a hazard. (The hazard is that encounter where the draft exceeds the depth.)

A vessel can survive in a failure state if it does not intersect a hazard. Interest lies only in the case where the infinite possible combinations of integrating the velocity vector result in the final position of the ship the same as the hazard:

$$\int_{t(\text{origin})}^{t(\text{destination})} v(t) dt = x_{\text{hazard}} - x_{\text{initial}} \quad (\text{B-1})$$

Given that the grounding failure state is the state of interest, the ship is following an unsafe track. Because the ship is proceeding down an unsafe track, there are two concerns to investigate:

1. The ship is able to follow a safe track
2. The ship is unable to follow a safe track.

If the ship is able to follow a safe track, then a determination must be made of why it is proceeding down an unsafe track. Figure B-1 depicts these concepts in the fault tree.

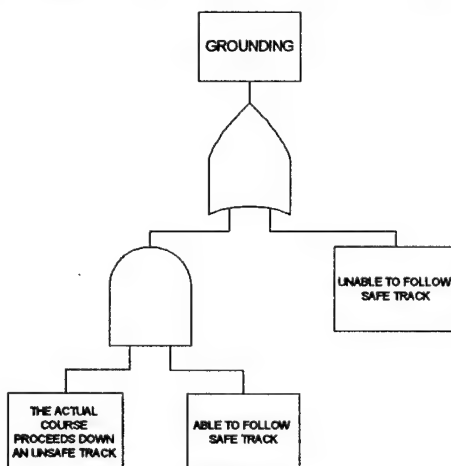


Figure B - 1: Basic Grounding Fault Tree



By deductively reducing each successive step in the top-down approach, the fundamental causes of groundings can be understood and evaluated. Continuing with these seemingly rudimentary steps in order to determine successive causes will create the complete fault tree. The process of developing the fault tree is subsequently described.

### **The Actual Course Follows an Unsafe Track**

The ship's actual course is following an unsafe track, yet there is nothing physically preventing the ship from following a safe track. Thus, two options can be deduced:

1. The desired track is unsafe.
2. The course has deviated from a desired safe track.

Given that the ship is capable of following a safe track, then, when the desired track intersects a hazard, causality is constrained to the planning process. However, when the ship's course deviates from a desired safe track to an unsafe track, causality is constrained to the piloting process.

### **The Desired Track is an Unsafe Track**

It is necessary to determine where in the planning process that the desired track becomes coincident with an unsafe track leading to a grounding. The coincidence of a desired track and a grounding track can occur under two different scenarios:

1. Properly planned track: the process of planning has been completed satisfactorily.
2. Improperly planned track: errors have occurred in the planning process

Planning includes both the initial voyage planning, and the dynamic planning which is done as a result of external conditions imposing new constraints.

The importance of proper planning can be illustrated through the use of the navigation control model. Clearly, if the ship navigation control system were completely accurate, then groundings would not occur due to deviations of the actual course from the desired track. But even accurate systems will yield an undesirable response if the input is incorrect. As the colloquialism goes "garbage in - garbage out." For example, a ship proceeding without the correct chart reflects an improper input to the control system. Regardless of how accurate the fix, if the intended track intersects an unknown hazard to navigation, the accuracy of the control system is irrelevant and the reliability of the system becomes limited by the reliability of the input.

Dynamic planning incorporates the same planning process, but it is done because some unanticipated event (weather, mechanical failure, another ship crossing the bow, etc.) has imposed new constraints upon the voyage. Dynamic planning is inherently a part of navigating

and piloting a ship. It often requires a rapid decision, and it is typically a quality of a skillful conning officer.

When the course is properly planned with all available information but still intersects a hazard, the fault lies in the information itself (e.g. incorrect charts). The planner has utilized the most current information and evaluated the intended tracks properly. But because the most current information does not reflect the most current conditions, the intended track intersects a grounding hazard.<sup>42</sup>

Groundings can and do occur due to inaccurate charts. Nautical charts are prepared from the latest available hydrographic surveys. Only a small portion of U.S. waters have been surveyed using the most advanced techniques, and 60 percent of the soundings shown on nautical charts are based on lead-line surveys conducted over 45 years ago [35].

For an improperly planned course, the voyage planning process has not been completed to success:

1. The wrong information is used: the correct information is available but is not used resulting in the wrong constraints placed upon the planning evaluation.
2. Insufficient information is used: the planning process is based upon incomplete knowledge of the voyage.

### **Actual Course Deviates from a Safe Desired Track**

The ship can be on the wrong course because it has deviated from the desired track. Recall from the navigation control model, in Figure 6-1, that deviations, which occur as the actual course diverges from the desired track, create error signals which the conning officer must recognize. The inaccuracy of the system is reflected when there is either a failure to recognize that the ship's actual position differs from its estimated position, or a difference in actual versus desired position results in insufficient action to eliminate the difference. After the difference is recognized, there must be an overt action to adjust the ordered course to keep the error as close to zero as possible.

Before proceeding any further it is necessary to review how a difference error is recognized. Most ships require a proactive interface between the sensors and the conning officer. The conning officer must take the initiative in the process. The proactive process of piloting a ship is dead-reckoning. Errors are detected by taking lines of position to fix the ship and compare the fix to the track. There will always be an error signal when the actual course deviates from the desired track. That signal may be masked by instrument error, or electrical/mechanical failure of navigation systems, but the error still exists and can be checked by visual lines of bearing to nav aids, or celestial fixes, etc.

---

<sup>42</sup> There are other issues involved with planning. For example, presenting the right information to the right person at the right time. The passage planner goes to great depth to develop a very detailed plan, which other people have to use. If the information is too cumbersome, then it will be ignored, if it is too detailed, then it can become irrelevant to a specific situation. This brings up the issue of contingency planning. Clearly, the planner cannot forecast every possible contingency. Therefore, this model simplifies the process by assuming that

The heart of navigation control model then, is the human decision process of determining if there is an error, and how much action is required to reduce the error. Given that an error exists in the difference between actual course and desired track, that error can either be detected or continue to go unrecognized.

If the difference error is not detected then causality is constrained to the fix or lack thereof. If the difference error is recognized, then there must be a determination of why insufficient action was taken.

### **The Difference Error is Recognized**

The possible actions which result in grounding after recognizing that the actual course differs from the desired track are:

1. Untimely action: the right action is taken but not in time to preclude an accident.
2. Erroneous action: the wrong action is taken.

It is assumed that all the information is available to the conning officer and the difference error is recognized in sufficient time to preclude a grounding. Hence, untimely or incorrect action in response to the difference error is either a failure of the conning officer to respond sufficiently to the error, or the helmsman to act promptly to the conning officer's orders.

### **The Difference Error is Not Recognized**

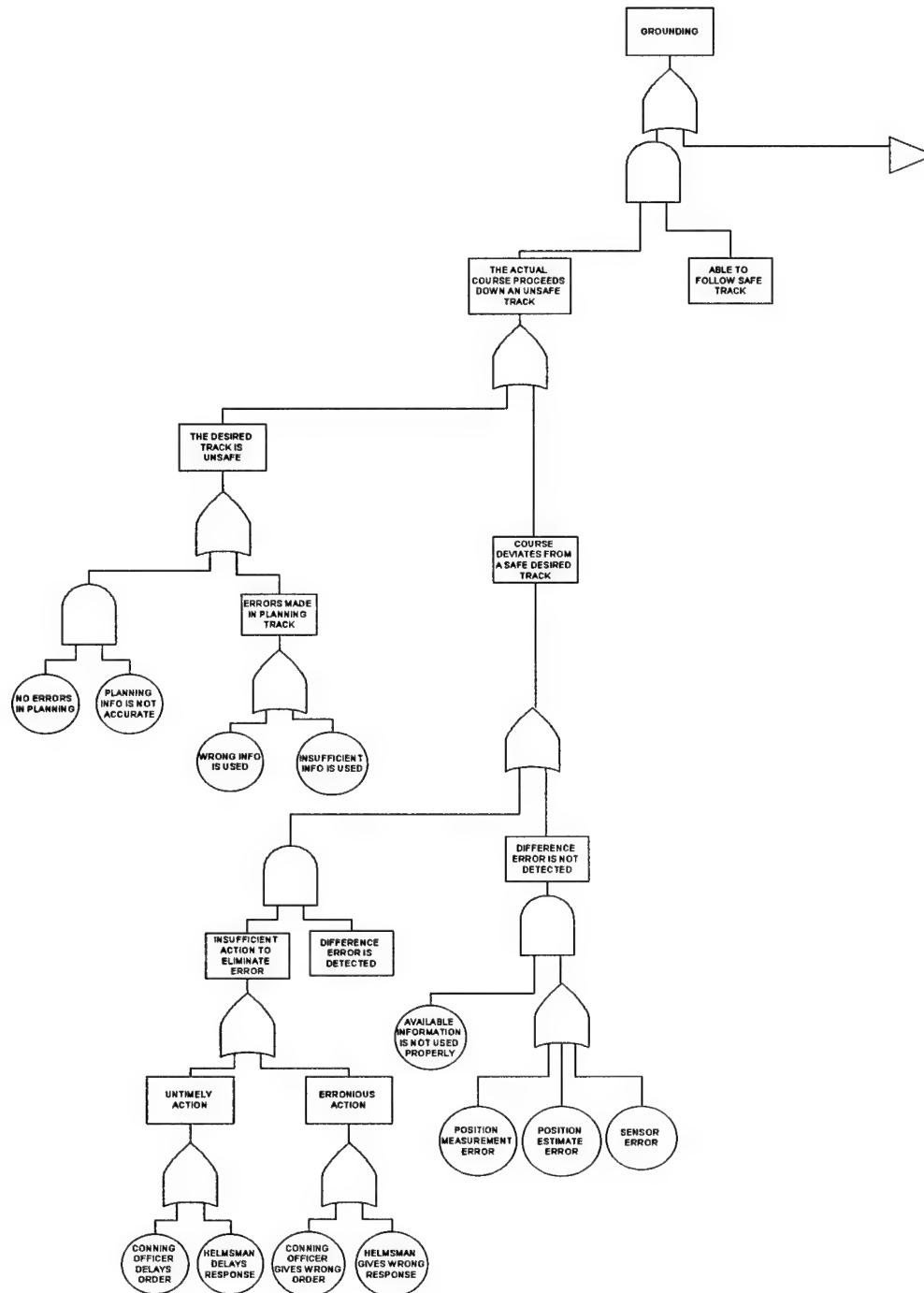
If the difference between the actual course and the desired track goes unrecognized, then the failure lies solely with the conning officer. Recall that the conning officer must compare all of the following:

1. Position Sensors: gyro, compass, lookout, radar errors.
2. Position Measurements: procedural errors in taking lines-of-position.
3. Position Estimates: procedural errors in dead-reckoning.

The breakdown in the loop occurs in the proactive process which must be initiated by the conning officer.

### **Summary of the Course Proceeding down an Unsafe Track**

Figure B-2 summarizes the fault tree for the actual course proceeding down an unsafe track. Basically, the faults occur because of either planning errors or piloting errors.



**Figure B - 2: Fault Tree for Actual Course Proceeding down an Unsafe Track**

## **Unable to Follow a Safe Track**

The correct course is known but the ship that is unable to steer that course. In this case, the ship is necessarily subjected to a number of parallel factors. All of the following must occur:

1. Lost way: the ship has lost its ability to be effectively controlled
2. Unsafe wind/current: when the ship has lost way, there must be the necessary wind/current to force the ship into the grounding situation.
3. Anchor failure: given that the ship is unable to dynamically control its course, the anchor must fail allowing the environment to control the inevitable.
4. Assistance failure: in addition to the above, there must be a failure of assistance to prevent the grounding.

## **The Ship has Lost Way**

For the ship to have lost way it is no longer able to be controlled. This would imply that the ship has lost steering or propulsion. Without getting into the details particular to a specific ship, failure of these mechanical systems can be attributed to maintenance, operation, or material failure. Additionally, given a material failure, the crew is unable to repair the failure before the ship intersects the hazard.

## **Unsafe Wind/Current**

For the ship to encounter a grounding given that it has lost way, it must be forced into the hazard by the wind/current. Many ships lose way while at sea, yet never encounter an accident. It is essential that the environment force the ship into the hazard for the hazard to occur.

## **Anchor Failure**

Tankers will have two anchors. Anchors on large tankers can weigh as much as 50,000 pounds each. But as ships have gotten larger, the anchors have not done so proportionately. The ratio of the anchor weight to the deadweight tonnage has dwindled from about 0.6 to 0.2 [7]. The anchors of large tankers are suitable for anchorage in designated areas, but with any significant way on the ship when dropping anchor, the momentum becomes too great for the anchors to handle.

As a mechanical system, the anchor system failure is subject to the same causality as the propulsion and steering systems; maintenance, operational, and material failure. Additionally, consideration should be made for the case when the anchor is not operated at all. Many vessels have run aground when prudent letting-go of the anchor would have prevented the catas-

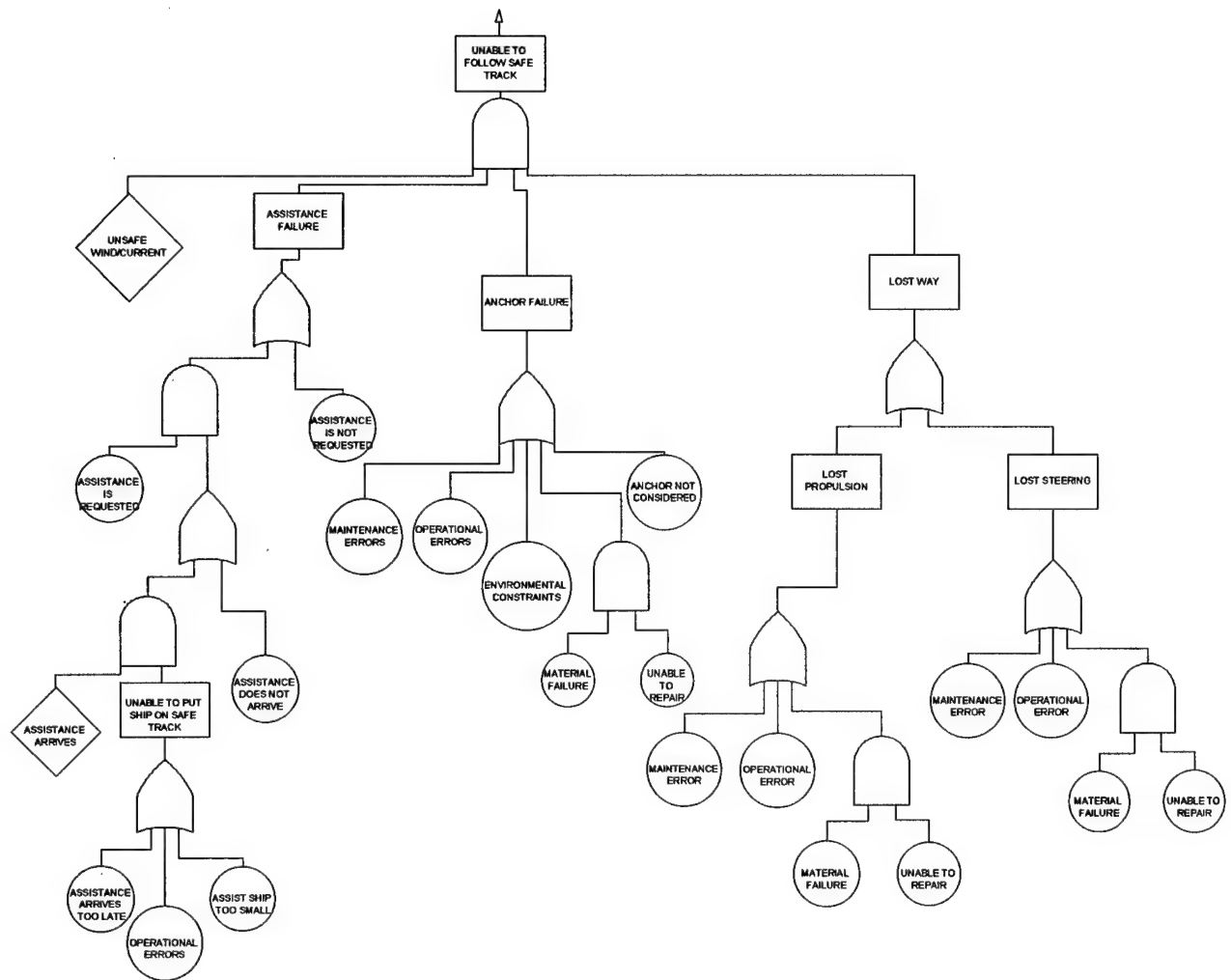
trophe. There are also times where the environmental conditions preclude effective anchor usage. The ocean bottom either does not lend it self to holding the anchor or the depth gradient is too steep.

### **Assistance Failure**

Tugs or salvage ships can be essential to preventing a catastrophe. The availability and functionality of assist ships is particular to a given port. Implicit failure of assistance occurs if it is not requested. Once requested, the failure can occur if the assistance does not arrive, or if the assistance is unable to put the ship on a safe track. The inability of the assist ship to put the damaged ship on a safe track can be caused by either the assist ship arriving too late, operational errors in securing a tow line, or the assist ship is too small to prevent the damaged ship from grounding.

### **Summary of Ship Unable to Follow a Safe Track**

Figure B-3 shows the fault tree for the grounding where the ship is unable to follow a safe track.



**Figure B - 3: Fault Tree For Ship Unable to Follow a Safe Track**

## Summary

The use of a fault tree to ascertain the areas of risk are essential to an overall risk assessment. Starting from the hazardous outcome, or top-event, and logically progressing downward through sequential levels of causation, the fault tree points to system weaknesses by deductively determining the sources. Once this systematic approach has developed all the root causes for groundings, the result is a qualitative assessment.

The fault tree is a way of decomposing the event, not a way of explaining why. As such, the grounding fault tree is a logical model representing a qualitative characterization of the system. The postulated fault events in the grounding fault tree are not exhaustive. Deductively and inductively, they represent the most likely events.

## Appendix C Selected THERP Tables

The following tables are excerpts of NUREG1278 [58]. They represent the tables used in the grounding analysis. They are supplied to give an illustration of the type of information in reference [58] and to show the source used for the analysis.

### Probabilities of Errors of Omission in Use of Written Procedures in Nonpassive Tasks

Task	HEP	Uncertainty
Errors of Comission	0.003	0.001 to 0.01
Procedures with checkoff provisions (assume zero dependence between written steps)		
Short list $\leq 10$ items	0.001	0.0005 to 0.005
Long list $\geq 10$ items	0.003	0.001 to 0.01
Checkoff provisions improperly used (Consider procedures with improperly used checkoff provisions to be the same as procedures with no checkoff provisions.)	0.5	0.1 to 0.9
Procedures with no checkoff provisions		
Short list $\leq 10$ items	0.003	0.0001 to 0.01
Long list $\geq 10$ items	0.01	0.005 to 0.05
Performance of simple arithmetic calculations	0.01	0.005 to 0.05
Procedures available but no used		
Maintenance tasks	0.3	0.05 to 0.9
Valve change or restoration tasks	0.01	0.005 to 0.05

### Probabilities of Error in Preparation of Written Procedures

Task	HEP	Uncertainty
Omitting an item	0.003	0.001 to 0.01
Writing an item incorrectly	0.003	0.001 to 0.01



### Probabilities that a Checker will Fail to Detect Errors

Checking Operation	HEP	Uncertainty
Usual monitoring in a nuclear power plant with some kind of checklist or written procedure (includes tasks such as over-the-shoulder checking and checking written lists or procedures)	0.10	0.05 to 0.5
Same as above but without written materials	0.20	0.10 to 0.9
Special short-term, one-of-a-kind checking (e.g., supervisor checks performance of a novice)	0.05	0.01 to 0.10
Hands-on type of checking that involves special measurements or other activities	0.01	0.005 to 0.05

### Probabilities of Errors of Commission in Reading Quantitative Information from Displays

Reading Task	HEP	Uncertainty
Digital indicators Analog meter	0.001	0.0005 to 0.005
Analog meters with easily seen limit marks	0.001	0.0005 to 0.005
Analog meters with difficult-to-see limit marks, such as scribe lines	0.002	0.001 to 0.01
Analog meters without limit marks	0.003	0.001 to 0.01
Analog-type chart recorders with limit marks	0.002	0.001 to 0.01
Analog-type chart recorders without limit marks	0.006	0.002 to 0.02
Checking the wrong indicator lamp (in an array of lamps)	0.003	0.001 to 0.01
Misinterpreting the indication on the indicator lamps	0.001	0.0005 to 0.005

### Probabilities of Errors in Recalling Special Instruction Items Given Orally

Task	HEP	Uncertainty
Items not Written Down by Recipient		
Recall any given item, given the following number of items to remember		
1	0.001	0.0005 to 0.005
2	0.003	0.001 to 0.01
3	0.01	0.005 to 0.05
4	0.03	0.01 to 0.1
5	0.1	0.05 to 0.5
Recall any item if supervisor checks to see that the task was done	-----	NEGLIGIBLE
Items Written Down by Recipient		
Recall any item (exclusive of errors in writing)	0.001	0.0005 to 0.005

## Appendix D Sensitivity Calculations

The following MATLAB program is used to determine the sensitivity of the event trees

```
% Ptrack = The probability that the desired track is unsafe
% Pinfo = The probability that the planning information is incorrect
% Pplan = The probability for implementing a faulty plan
% Ppilot = The probability of a piloting error

% The events for passage planning are as follows
% chk_pub = check publications
% plt_chg = plot changes
% det_wpt = determine waypoints
% lay_trk = lay down track
% recflt = recognize faulty track
% ver_pln = captain properly verifies plan

% The events for piloting are as follows
% err_gen = the probability that a difference error is generated
% fix_tak = the probability that a fix is taken
% fix_plt = the probability that a fix is plotted properly
% fix_ver = the probability that the fix is verified to be correct
% cov_fix = the probability that the captain verifies the fix to be correct
% dif_det = the probability that the difference error is detected
% co_detd = the probability that the captain detects the difference
% crs_ord = the probability that the correct coarse change is ordered
% crs_ver = the probability that the coarse change is verified
% cov_crs = the probability the captain verifies the coarse change
% hlm_res = the probability that the helm responds correctly
% hlm_ver = the probability that the helm response is verified
% cov_hlm = the probability that the captain verifies the helm response

% The failure probabilities are as follows:
nchk_pub = 0.003;
nplt_chg = 0.001;
ndet_wpt = 0.003;
nlay_trk = 0.01;
nrecflt = 0.002;
nver_pln = 0.01;
Pinfo= 0.0001;

nerr_gen = 0.00095;
nfix_tak = 0.001;
nfix_plt = 0.001;
nfix_ver = 0.01;
ncov_fix = 0.01;
ndif_det = 0.001;
```

```

nco_detd = 0.001;
ncrs_ord = 0.003;
ncrs_ver = 0.01;
ncov_crs = 0.01;
nhlm_res = 0.0001;
nhlm_ver = 0.01;
ncov_hlm = 0.01;

```

```

% The success probabilities are 1-Pfailure

```

```

format short e;
global chk_pub plt_chg det_wpt lay_trk recflt ver_pln
global nchk_pub nplt_chg ndet_wpt nlay_trk nrecflt nver_pln
global Pplan
global err_gen fix_tak fix_plt fix_ver cov_fix dif_det co_detd crs_ord crs_ver
global cov_crs hlm_res hlm_ver cov_hlm
global nerr_gen nfix_tak nfix_plt nfix_ver ncov_fix ndif_det nco_detd ncrs_ord ncrs_ver
global ncov_crs nhlm_res nhlm_ver ncov_hlm
global Ppilot

```

```

% check the sensitivity for the events in the planning event tree
% plan is called as a function
% plan computes the probability from the event tree

```

```

plan;
Planinit(:)=[Pplan,Pplan]

```

```

nchk_pub=[0.001;0.01];
plan;
Plan(:,1)=Pplan;
nchk_pub=0.003;

```

```

nplt_chg=[0.0005;0.005];
plan;
Plan(:,2)=Pplan;
nplt_chg=0.001;

```

```

ndet_wpt=[0.001;0.01];
plan;
Plan(:,3)=Pplan;
ndet_wpt=0.003;

```

```

nlay_trk=[0.005;0.05];
plan;
Plan(:,4)=Pplan;
nlay_trk=0.01;

```

```

nrecflt=[0.001;0.01];
plan;
Plan(:,5)=Pplan;
nrecflt=0.002;

```

```

nver_pln=[0.005;0.5];
plan;
Plan(:,6)=Pplan;
nver_pln=0.01;

%incorporate the probability of faulty information to determine the
%sensitivity of the probability for implementing a faulty track

plan;
Ptrackinit(:)=[Pplan+Pinfo,Pplan+Pinfo]

nchk_pub=[0.001;0.01];
plan;
Ptrack(:,1)=Pplan+Pinfo;
nchk_pub=0.003;

nplt_chg=[0.0005;0.005];
plan;
Ptrack(:,2)=Pplan+Pinfo;
nplt_chg=0.001;

ndet_wpt=[0.001;0.01];
plan;
Ptrack(:,3)=Pplan+Pinfo;
ndet_wpt=0.003;

nlay_trk=[0.005;0.05];
plan;
Ptrack(:,4)=Pplan+Pinfo;
nlay_trk=0.01;

nrecflt=[0.001;0.01];
plan;
Ptrack(:,5)=Pplan+Pinfo;
nrecflt=0.002;

nver_pln=[0.005;0.5];
plan;
Ptrack(:,6)=Pplan+Pinfo;
nver_pln=0.01;

Pinfo=[0.00001;0.001];
plan;
Ptrack(:,7)=Pplan+Pinfo;
Pinfo=0.0001;

%pilot is called as a function
%pilot determines the probability from the event tree

pilot;
Pilotinit(:) = [Ppilot,Ppilot]

```

```
nerr_gen = [0.000001;0.001];  
pilot;  
Pilot(:,1)=Ppilot;  
nerr_gen = 0.00095;
```

```
nfix_tak = [0.0005;0.005];  
pilot;  
Pilot(:,2)=Ppilot;  
nfix_tak=0.001;
```

```
nfix_plt = [0.0005;0.005];  
pilot;  
Pilot(:,3)=Ppilot;  
nfix_plt=0.001;
```

```
nfix_ver = [0.005;0.05];  
pilot;  
Pilot(:,4)=Ppilot;  
nfix_ver=0.01;
```

```
ncov_fix = [0.005;0.05];  
pilot;  
Pilot(:,5)=Ppilot;  
ncov_fix=0.01;
```

```
ndif_det = [0.0005;0.005];  
pilot;  
Pilot(:,6)=Ppilot;  
ndif_det=0.001;
```

```
nco_detd = [0.0005;0.005];  
pilot;  
Pilot(:,7)=Ppilot;  
nco_detd=0.001;
```

```
ncrs_ord = [0.001;0.01];  
pilot;  
Pilot(:,8)=Ppilot;  
ncrs_ord=0.003;
```

```
ncrs_ver = [0.005;0.05];  
pilot;  
Pilot(:,9)=Ppilot;  
ncrs_ver=0.01;
```

```
ncov_crs = [0.005;0.05];  
pilot;  
Pilot(:,10)=Ppilot;  
ncov_crs=0.01;
```

```
nhlm_res = [0.00005;0.0005];  
pilot;  
Pilot(:,11)=Ppilot;
```

```

nhlm_res=0.0001;

nhlm_ver = [0.005;0.05];
pilot;
Pilot(:,12)=Ppilot;
nhlm_ver=0.01;

ncov_hlm = [0.005;0.05];
pilot;
Pilot(:,13)=Ppilot;
ncov_hlm=0.01;

%pilot2 determines the probability from the event tree without captain verification

pilot2;
Pilotinit(:) = [Ppilot,Ppilot]

nerr_gen = [0.000001;0.001];
pilot2;
Pilot(:,1)=Ppilot;
nerr_gen = 0.00095;

nfix_tak = [0.0005;0.005];
pilot2;
Pilot(:,2)=Ppilot;
nfix_tak=0.001;

nfix_plt = [0.0005;0.005];
pilot2;
Pilot(:,3)=Ppilot;
nfix_plt=0.001;

nfix_ver = [0.005;0.05];
pilot2;
Pilot(:,4)=Ppilot;
nfix_ver=0.01;

ncov_fix = [0.005;0.05];
pilot2;
Pilot(:,5)=Ppilot;
ncov_fix=0.01;

ndif_det = [0.0005;0.005];
pilot2;
Pilot(:,6)=Ppilot;
ndif_det=0.001;

ncrs_ord = [0.001;0.01];
pilot2;
Pilot(:,7)=Ppilot;
ncrs_ord=0.003;

ncrs_ver = [0.005;0.05];

```

```
pilot2;  
Pilot(:,8)=Ppilot;  
ncrs_ver=0.01;
```

```
ncov_crs = [0.005;0.05];  
pilot2;  
Pilot(:,9)=Ppilot;  
ncov_crs=0.01;
```

```
nhlm_res = [0.00005;0.0005];  
pilot2;  
Pilot(:,10)=Ppilot;  
nhlm_res=0.0001;
```

```
nhlm_ver = [0.005;0.05];  
pilot2;  
Pilot(:,11)=Ppilot;  
nhlm_ver=0.01;
```

```
ncov_hlm = [0.005;0.05];  
pilot2;  
Pilot(:,12)=Ppilot;  
ncov_hlm=0.01;
```

```
%the results are written to an output file
```

```
diary sense.out;
```

```
Pilotinit  
Pilot'  
diary off;
```

function plan

```
chk_pub = 1-nchk_pub;  
plt_chg = 1-nplt_chg;  
det_wpt = 1-ndet_wpt;  
lay_trk = 1-nlay_trk;  
rec_flt = 1-nrec_flt;  
ver_pln = 1-nver_pln;
```

```
Pplan = chk_pub * plt_chg * det_wpt * nlay_trk * nrec_flt * nver_pln...  
+ chk_pub * plt_chg * ndet_wpt * nver_pln...  
+ chk_pub * nplt_chg * det_wpt * lay_trk * nver_pln...  
+ chk_pub * nplt_chg * det_wpt * nlay_trk * rec_flt * nver_pln...  
+ chk_pub * nplt_chg * det_wpt * nlay_trk * nrec_flt * nver_pln...  
+ chk_pub * nplt_chg * ndet_wpt * nver_pln...  
+ nchk_pub * det_wpt * lay_trk * nver_pln...  
+ nchk_pub * det_wpt * nlay_trk * rec_flt * nver_pln...  
+ nchk_pub * det_wpt * nlay_trk * nrec_flt * nver_pln...  
+ nchk_pub * ndet_wpt * nver_pln;
```



function pilot

```
err_gen = 1-nerr_gen;
fix_tak = 1-nfix_tak;
fix_plt = 1-nfix_plt;
fix_ver = 1-nfix_ver;
cov_fix = 1-ncov_fix;
dif_det = 1-ndif_det;
co_detd = 1-nco_detd;
crs_ord = 1-ncrs_ord;
crs_ver = 1-ncrs_ver;
cov_crs = 1-ncov_crs;
hlm_res = 1-nhlm_res;
hlm_ver = 1-nhlm_ver;
cov_hlm = 1-ncov_hlm;
Pa=err_gen * fix_tak * fix_plt * dif_det * crs_ord *      nhlm_res * nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * fix_plt * dif_det * ncrs_ord * crs_ver *      nhlm_res * nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * fix_plt * dif_det * ncrs_ord * ncrs_ver * cov_crs * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * fix_plt * dif_det * ncrs_ord * ncrs_ver * ncov_crs...
+ err_gen * fix_tak * fix_plt * ndif_det;

Pb=err_gen * fix_tak * nfix_plt * fix_ver * dif_det * crs_ord *      nhlm_res * nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * nfix_plt * fix_ver * dif_det * ncrs_ord * crs_ver *      nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * fix_ver * dif_det * ncrs_ord * ncrs_ver * cov_crs * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * fix_ver * dif_det * ncrs_ord * ncrs_ver * ncov_crs...
+ err_gen * fix_tak * nfix_plt * fix_ver * ndif_det;

Pc=err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * crs_ord * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * ncrs_ord * crs_ver * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * ncrs_ord * ncrs_ver * cov_crs * nhlm_res *
nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * ncrs_ord * ncrs_ver * ncov_crs...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * ndif_det...
+ err_gen * fix_tak * nfix_plt * nfix_ver * ncov_fix...
+ err_gen * nfix_tak...
+ nerr_gen;

Ppilot = Pa + Pb + Pc;
```

function pilot2

```

Pa=err_gen * fix_tak * fix_plt * dif_det * crs_ord *      nhlm_res * nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * fix_plt * dif_det * ncrs_ord * crs_ver *      nhlm_res * nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * fix_plt * dif_det * ncrs_ord * ncrs_ver * cov_crs * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * fix_plt * dif_det * ncrs_ord * ncrs_ver * ncov_crs...
+ err_gen * fix_tak * fix_plt * ndif_det;

```

```

Pb=err_gen * fix_tak * nfix_plt * fix_ver * dif_det * crs_ord *      nhlm_res * nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * nfix_plt * fix_ver * dif_det * ncrs_ord * crs_ver *      nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * fix_ver * dif_det * ncrs_ord * ncrs_ver * cov_crs * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * fix_ver * dif_det * ncrs_ord * ncrs_ver * ncov_crs...
+ err_gen * fix_tak * nfix_plt * fix_ver * ndif_det;

```

```

Pc=err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * crs_ord * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * ncrs_ord * crs_ver * nhlm_res * nhlm_ver *
ncov_hlm...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * ncrs_ord * ncrs_ver * cov_crs * nhlm_res *
nhlm_ver * ncov_hlm...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * dif_det * ncrs_ord * ncrs_ver * ncov_crs...
+ err_gen * fix_tak * nfix_plt * nfix_ver * cov_fix * ndif_det...
+ err_gen * fix_tak * nfix_plt * nfix_ver * ncov_fix...
+ err_gen * nfix_tak...
+ nerr_gen;

```

Ppilot = Pa + Pb + Pc;

## Bibliography

- [1] Amrozowicz, M.D., "The Need for a Probabilistic Risk Assessment of the Oil Tanker Industry and a Qualitative Assessment of Oil Tanker Groundings," Master of Engineering Thesis, Department of Ocean Engineering, Massachusetts Institute of Technology, January, 1996.
- [2] Bea R.G., Roberts K., "Management of Rapidly Developing Crises: A Multi-Community Study," Presented at the American Petroleum Institute Sixth Crisis Seminar, Houston TX, September 25-27, 1995.
- [3] Bea R.G., *The Role of Human Error in Design, Construction, and Reliability of Marine Structures*, Ship Structures Committee, SSC-378, November, 1994.
- [4] Bea R.G., Moore W.H., "Reliability Based Evaluations of Human and Organization Errors in Reassessment & Requalification of Platforms," International Offshore Mechanics and Arctic Engineering Conference Safety and Reliability Symposium, No. OMAE 94-1272, February, 1994.
- [5] Bea R.G., Moore W.H., "Operational Reliability and Marine Systems," *New Challenges to Understanding Organizations*, Roberts K.H., Macmillan Publishing Company, New York, 1993.
- [6] Bea R.G., "Human and Organization Factors in the Safety of Offshore Structures," *Risk and Reliability in Marine Technology*, Balkema Publisher, Rotterdam, The Netherlands.
- [7] Cahill R.A., *Disasters at Sea: Titanic to Exxon Valdez*, Nautical Books, San Antonio, 1991.
- [8] Department of Transportation, U.S. Coast Guard, *Prevention Through People: Quality Action Team Report*, U.S. Coast Guard Office of Marine Safety, Security and Environmental Protection, Office of Navigation, Safety and Waterways Services, July 15, 1995.
- [9] Department of Transportation, U.S. Coast Guard Research and Development Center and Marine Safety International Computer Aided Operations Research Facility, *Human Factors Evaluation of Electronic Chart Display and Information Systems (ECDIS)*, Report No. CG-D-12-95, U.S. Coast Guard Office of Engineering, Logistics, and Development, Washington DC, February, 1995.
- [10] Department of Transportation, U.S. Coast Guard, *Report of the Tanker Safety Study Group*, October 6, 1989.

- [11] DNV Technica, *Risk Analysis of Oil Spills from Tankers in UK Waters*, Prepared for Marine Pollution Control Unit, UK CoastGuard, Det Norske Veritas Industry LTD., May, 1995.
- [12] Dougherty E. M., Fragola J. R. *Human Reliability Analysis*, John Wiley & Sons, New York, 1988.
- [13] Drewry Shipping Consultants LTD., *Deep-Sea Towage, Salvage and Heavy Lift Markets*, Drewry Shipping Consultants LTD., 1992.
- [14] Farrington J.W. "Oil Pollution: A Decade of Research and Monitoring," *Oceanus* Vol. 28 No.3, Fall, 1985.
- [15] Fishcoff B., "Hindsight Does not Equal Foresight: The Effect of Outcome Knowledge on Judgement Under Uncertainty," *Journal of Experimental Psychology: Human Performance and Perception*, 1, 1975.
- [16] Gardenier J.S., "Ship Navigational Failure Detection and Diagnosis," *Human Detection and Diagnosis of System Failures*, Edited by Rasmussen J., Rouse W.B., Plenum Press, New York, 1980.
- [17] Gertman D.I., Blackman H.S., *Human Reliability & Safety Analysis Data Handbook*, John Wiley & Sons, Inc., New York, 1994.
- [18] Gonin I.M., Dowd M.K., "1993 At-Sea Evaluation of ECDIS," *Journal of The Institute of Navigation*, Vol. 41, No. 4, Winter 1994-1995.
- [19] Grabowski M.R., Sanquist T.F., *Alaska Maritime Human Factors Needs Assessment*, Submitted to Cook Inlet and Prince William Sound Regional Citizens Advisory Councils, September 23, 1994.
- [20] Groeneweg J., *Controlling the Controllable*, DSWO Press, Leiden University, The Netherlands, 1994.
- [21] Grose V.L., "Technology's Impact on Human Risk," *Proceedings of the Marine Safety Council*, May-June 1995.
- [22] Hollnagel E., *Human Reliability Analysis: Context and Control*, Academic Press, San Diego, 1993.
- [23] International Maritime Organization, *International Safety Management Code (ISM Code)*, IMO, London, 1994.

- [24] International Maritime Organization, *International Convention for the Safety of Life at Sea*, IMO, London, 1986.
- [25] The Institute of London Underwriters, *The Institute of London Underwriters 1992 Casualty Statistics*, 1992.
- [26] Jones R.B., "The Enemy from Within," *Proceedings of the Marine Safety Council*, May-June, 1995.
- [27] Jukola H., Castleman G.E., "Z-Drive Escort Tug Operating Modes," *Marine Technology*, Vol. 32, No. 3, July, 1995.
- [28] Kristiansen I.S., Rensvik E., "Human and Organisational Factors in Safe Operation and Pollution Prevention," IMAS 92, Quality of Shipping in the Year 2000, Paper 12, November, 1992.
- [29] Lamb B.L., Boyet D.M., "An Update on the Oil Pollution Act of 1990," *Marine Technology*, Vol. 32, No. 2, April, 1995.
- [30] Lowry I.J., "Improving Mariner/Ship Interaction," *Marine Technology*, Vol 31, No.2, April 1994.
- [31] Maloney E.S., *Dutton's Navigation & Piloting*, Naval Institute Press, Annapolis, 1985.
- [32] Mannschreck W.A., *Analysis of Surface Ship Mishaps*, Naval Safety Center, Naval Air Station Norfolk,
- [33] Modarress, M. *What Every Engineer Should Know About Reliability and Risk Analysis*, Marcel Dekker, Inc., New York, 1993.
- [34] Moore W.H., Bea R.G., "Management of Human and Organisational Error Throughout a Ship's Life Cycle," Paper 18, IMAS95, Management and Operation of Ships: Practical Techniques for Today and Tomorrow, The Institute of Marine Engineers, May 24-25, 1995.
- [35] National Research Council, Committee on Advances in Navigation and Piloting, Marine Board, *Minding the Helm, Marine Navigation and Piloting*, National Academy of Sciences, National Academy Press, Washington D.C., 1994.
- [36] National Research Council, Committee on Tank Vessel Design, *Tanker Spills: Prevention by Design*, National Academy of Sciences, National Academy Press, Washington D.C., 1991.
- [37] National Research Council, Committee on the Effect of Smaller Crews on Maritime Safety, Marine Board, *Crew Size and Maritime Safety*, Commission on Engineering and

Technical Systems, National Academy of Sciences, National Academy Press, Washington D.C., 1990.

[38] National Research Council, Panel on Human Error in Merchant Marine Safety, Maritime Transportation Research Board, *Human Error in Merchant Marine Safety*, National Academy of Sciences, National Academy Press, Washington D.C., 1976.

[39] Notthoff A., "Spill Sparks Reform, Leaves Lasting Scar," *Forum for Applied Research and Public Policy*, Winter, 1991.

[40] Norman D. A., *The Design of Everyday Things*, Doubleday, New York, 1990.

[41] Pedersen P.T., "Collision and Grounding Mechanics," Paper presented at WEMT 95 - Ship Safety and Protection of the Environment, 1992.

[42] Perrow, C., *Normal Accidents*, Basic Books, New York 1984.

[43] Peters H.J., *The International Ocean Transport Industry in Crisis: Assessing the Reasons and Outlook*, Policy Research Working Papers, Transport, Water, and Urban Development Department, The World Bank, WPS 1128, April, 1993.

[44] Ramakumar R., *Engineering Reliability: Fundamentals and Applications*, Prentice-Hall, Englewood Cliffs, New Jersey, 1993.

[45] Rasmussen N.C., *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington D.C., October, 1975.

[46] Reason J., *Human Error*, Cambridge University Press, Cambridge, 1990.

[47] Robert Allan LTD, *Study of Emergency Towing Services Worldwide*, Prepared for the Washington State Office of Marine Safety, Robert Allan LTD Naval Architects and Marine Engineers, Project 15-94, Vancouver, June 13, 1994.

[48] Robert Allan LTD, *Cost Analysis of an Emergency Towing System*, Prepared for the Washington State Office of Marine Safety, Robert Allan LTD Naval Architects and Marine Engineers, Project 107-93, Vancouver, March, 1994.

[49] Robert Allan LTD, *The Role and Benefits of Escort Tugs in Canadian Waters*, Robert Allan LTD Naval Architects and Marine Engineers, Vancouver, January, 1994.

[50] Sanders M.S., McCormick E.J., *Human Factors in Engineering and Design*, McGraw-Hill Book Company, New York, 1987.

- [51] Singh S.J., "Human Error in Collisions and Groundings of Ships," Paper presented at The Center for Maritime Education, Training and the Human Element in Accident Prevention, October 11-13, 1995.
- [52] Singh S.J., "The Aetiology of Grounding," Ph D. Thesis, University of Wales, College of Cardiff, Department of Maritime Studies & International Transport, March 1995.
- [53] Singh S.J., "The Maritime Transportant and the Maritime Malaise," Unpublished, 1993.
- [54] Singh S.J., "Ports and Ships--A Technological Intervention," Unpublished, 1991.
- [55] Siu N.O., Novack S.D., Hill S.G., Bhimavarapu K.R., *Evaluating Risk Assessment Approaches in Oil Spill Prevention Applications*, INEL-95/0401, Idaho National Engineering Laboratory, Engineering Analysis Department, Idaho Falls, August, 1995.
- [56] Smith M.W., Akerstron-Hoffman R., Pizzariello C.M., Siegel S.I., Schreiber T.E., Gonin I.M., "The Mariner's Use of Automated Navigation Systems," U.S. Coast Guard Research and Development Center, Prepared for the Transportation Resarch Board Meeting, Washington DC, January 1994.
- [57] Stainer M., Lim C.Y., Sherman J., "Maritime Transportation Initiating Coverage: Investing in a Global Industry," U.S. Investment Research, Morgan Stanley Research, November 7, 1995.
- [58] Swain, A.D., Guttman, H.E., *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington D.C., 1983.
- [59] Townsend R., Glazer M., *Safe Passage: Preventing Oil Spills in our Marine Sanctuaries*, Center for Marine Conservation, Inc., Pacific Region, San Francisco, 1994.
- [60] United Kingdom Protection and Indemnity Club, *Analysis of Major Claims 1993*, The United Kingdom Mutual Steam Ship Assurance Association (Bermuda) LTD, 1993.
- [61] United Kingdom Protection and Indemnity Club, *The Human Factor: A report on Manning*, UK P&I Club.
- [62] United Nations Conference on Trade and Development, *Review of Maritime Transport 1992*, United Nations, New York, 1993.
- [63] United Nations Conference on Trade and Development, *Review of Maritime Transport 1993*, United Nations, New York, 1994.

[64] United States Army Corps of Engineers, *Waterborne Commerce of the United States, Waterways and Harbors*, (Excerpts from 1986 - 1990 received from U.S. ACOE Waterborne Commerce Statistics Center)

[65] von Zharen W.M., Duncan W., "Environmental Risk Assessment and Management in the Maritime Industry: The Interaction with ISO 9000, ISM and ISM Management Systems," Annual Meeting of The Society of Naval Architects and Marine Engineers, No. 7, 1994.

[66] Washington State Office of Marine Safety, *An Oil Spill Prevention Proposal for a Dedicated Rescue Tug to Protect the Strait of Juan De Fuca and Adjacent Pacific Coast*, Final Report of the Emergency Towing System Task Force, August, 1993.

[67] Woods Hole Oceanographic Institution, Marine Policy Center, *A Model of Transit Risk and Application to the Prioritization of Hydrographic Surveys*, Proposal submitted to the Sea Grant Program, Massachusetts Institute of Technology, February, 1995.